50 CLÉS POUR COMPRENDRE LES MATHS

TONY
CRILLY



DUNOD

50 CLÉS POUR COMPRENDRE LES MATHS

TONY
CRILLY

Traduit de l'anglais par Véronique Bordellès

DUNOD

Table des matières

Introduction

Les mathématiques sont un vaste domaine que nul ne peut maîtriser entièrement. Ce que l'on peut faire en revanche, c'est trouver son propre chemin pour les explorer. Les possibilités qui nous sont offertes nous entraîneront alors vers d'autres époques et des cultures différentes, nous faisant ainsi découvrir des idées qui ont plongé les mathématiciens dans la perplexité pendant des siècles.

Les mathématiques sont une discipline à la fois ancienne et moderne et se sont édifiées à partir d'influences culturelles et politiques venues du monde entier. Les Indiens et les Arabes nous ont donné notre système de numération actuel que viennent cependant émailler quelques vestiges du passé. Nous retrouvons encore des traces de la base « 60 » des Babyloniens des 2e et 3e millénaires av. J.-C. Ainsi, il y a 60 secondes dans 1 minute et 60 minutes dans 1 heure, un angle droit fait toujours 90° et non pas 100 grades en dépit de la tentative de la France révolutionnaire d'imposer le système décimal.

Les triomphes technologiques de l'époque moderne sont liés aux mathématiques, ce qui fait qu'aujourd'hui, on ne peut certainement plus se vanter d'avoir été un élève médiocre dans cette matière. Bien sûr, les mathématiques de l'école sont différentes car souvent enseignées dans le seul but de préparer à des examens. Le rythme soutenu imposé aux élèves n'est pas non plus propice à son enseignement, car les mathématiques sont une matière pour laquelle on ne gagne pas à être rapide. Il faut du temps pour apprivoiser les idées. Certains des plus grands mathématiciens ont fait preuve d'une lenteur monumentale dans leurs efforts pour comprendre les concepts compliqués qu'ils étudiaient.

Inutile, donc, de se précipiter pour lire ce livre. On peut le feuilleter à loisir. Prenez le temps de découvrir le sens réel de ces idées dont vous avez peut-être déjà entendu parler. Commencez par le chapitre sur le chiffre zéro, ou un autre si vous voulez, et de là, vous pouvez partir à la découverte des terres de la pensée mathématique. Vous pouvez, par exemple, vous informer sur la théorie des jeux, puis lire le chapitre sur les carrés magiques. Ou alors, après avoir vu les rectangles d'or, vous pouvez aller au grand théorème de Fermat, ou n'importe où ailleurs.

Nous vivons une époque passionnante pour les mathématiques. Ces dernières années, quelques-uns des plus grands problèmes ont été résolus. Les développements modernes de l'informatique ont permis d'en résoudre certains, mais se sont avérés impuissants pour en résoudre d'autres. La solution au problème des quatre couleurs a été trouvée grâce à l'ordinateur, mais l'hypothèse de Riemann, sujet du chapitre final de cet ouvrage, n'est toujours pas démontrée, que ce soit avec un ordinateur ou par un autre moyen.

Les mathématiques s'adressent à tous. La popularité du sudoku est la preuve que l'on peut faire des mathématiques (sans le savoir) et en plus y prendre du plaisir. Les mathématiques, comme l'art ou la musique, ont connu des génies dont l'histoire ne résume pas tout. Vous verrez plusieurs éminents personnages faire leur entrée et leur sortie dans certains chapitres puis revenir dans d'autres. Leonhard Euler, dont le tricentenaire a eu lieu en 2007, apparaît régulièrement dans ces pages. On doit cependant les vrais progrès des mathématiques à cette « multitude obscure » dont les travaux se sont accumulés au cours des siècles. Ce choix, certes personnel, de 50 sujets a toutefois été guidé par le désir de respecter un certain équilibre. Vous trouverez des thèmes familiers et d'autres plus poussés, des mathématiques pures et appliquées, abstraites et concrètes, anciennes et modernes. Les mathématiques forment cependant un tout, et la difficulté n'a donc pas été de choisir les sujets mais d'en éliminer certains. Il aurait pu y avoir 500 idées, mais 50 suffisent largement pour vous permettre de faire de bons débuts dans le monde mathématique.

01 Zéro

Tout petits, c'est d'un pas mal assuré que nous faisons notre entrée au pays des nombres. On nous y apprend que le 1 occupe la première position dans « l'alphabet des nombres », et qu'il est suivi de 2, 3, 4, 5… Les nombres ne servent à rien d'autre qu'à compter des choses réelles telles que des pommes, des oranges, des bananes, des poires. Ce n'est que bien plus tard que l'on apprend à compter le nombre de pommes dans une boîte lorsque celle-ci est vide.

Les Grecs de l'Antiquité eux-mêmes, qui ont pourtant permis l'avancée prodigieuse des sciences et des mathématiques, et qui se sont illustrés par leurs prouesses dans le domaine de la technologie, ne disposaient d'aucune méthode efficace pour compter le nombre de pommes dans une boîte vide. Ils n'ont pas réussi à donner un nom au « rien ». Les Romains avaient quant à eux une façon très particulière de combiner I, V, X, L, C, D et M. Mais qu'en était-il du 0 ? Ils ne comptaient pas le « rien ».

Comment le zéro est-il parvenu à se faire accepter ? L'utilisation d'un symbole pour désigner « le néant » remonterait à des milliers d'années. La civilisation Maya qui occupait le Mexique actuel employait le zéro sous différentes formes. Un peu plus tard, l'astronome Claudius Ptolémée, influencé par les Babyloniens, utilisait un symbole proche de notre 0 pour marquer une position dans son système de numération. En tant que marqueur de position, le zéro pouvait servir à différencier des nombres tels que 75 et 705 par exemple, sans avoir besoin de se référer au contexte comme le faisaient les Babyloniens. C'est un peu comme la « virgule » dans le langage écrit : tous deux nous permettent de « lire » la bonne signification. Toutefois, de même que l'utilisation de la virgule est accompagnée d'un ensemble de lois, des règles sont nécessaires pour bien utiliser le zéro.

Le mathématicien indien Brahmagupta au VIIe siècle de notre ère, pour qui le zéro était un « nombre » comme les autres, avait fixé des règles pour l'utiliser. Selon l'une d'elles, « la somme d'un nombre positif et de zéro est positive » et « la somme de zéro plus zéro est égale à zéro ». En considérant zéro comme un nombre et non pas seulement comme un marqueur de position, il était en avance sur son temps. Le système de numération indo-arabe dans lequel le zéro était utilisé comme un nombre fut diffusé en occident par Léonard de Pise, plus connu sous le nom de Fibonacci,

chronologie

700 av. J.-C.
Les Babyloniens utilisent le zéro en tant que marqueur de position dans leur système de numération.

628 av. J.-C.
Brahmagupta utilise le zéro et fixe des règles pour l'utiliser avec les autres chiffres.

dans son ouvrage intitulé *Liber Abaci* (*Le Livre des abaques*) qu'il publia en 1202. Élevé en Afrique du Nord et formé à l'école arithmétique indo-arabe, il reconnaissait tout l'intérêt qu'il y avait à utiliser le signe supplémentaire 0 en combinaison avec les symboles indiens 1, 2, 3, 4, 5, 6, 7, 8 et 9.

L'introduction du zéro dans le système de numération posa un problème que Brahmagupta n'examina que rapidement : comment fallait-il traiter cet « intrus » ? Il esquissa une solution, mais les expédients qu'il proposait étaient vagues. Comment faire pour réellement intégrer le zéro dans le système arithmétique existant ? Certains ajustements étaient simples. Tant qu'il s'agissait d'additionner et de multiplier, 0 s'intégrait parfaitement, mais les opérations de soustraction et de division s'entendaient mal avec « l'étranger ». Des simplifications étaient nécessaires pour permettre au 0 de s'accorder avec l'arithmétique pratiquée à l'époque.

Comment fonctionne le zéro ? Les additions et les multiplications avec zéro sont simples et ne donnent pas lieu à contestation. Si 0 vient s'ajouter à 10, on obtient 100, mais « ajouter » doit être pris ici dans un sens purement numérique. additionner 0 à un nombre le laisse inchangé alors que multiplier 0 par n'importe quel nombre donne toujours 0. Par exemple, on a $7 + 0 = 7$ et $7 \times 0 = 0$. La soustraction est une opération simple qui peut cependant donner des nombres négatifs, $7 - 0 = 7$, et $0 - 7 = -7$, alors que la division avec 0 est source de difficultés.

Imaginons qu'il nous faille mesurer une longueur donnée avec une règle. Supposons que cette règle est de sept unités de long. Nous voulons savoir combien de règles nous pouvons mettre bout à bout pour effectuer notre mesure. Si notre longueur est de 28 unités effectives, la réponse est 28 divisé par 7 ou, avec les symboles mathématiques, $28 \div 7 = 4$. On préfère noter cette division sous la forme

$$\frac{28}{7} = 4$$

On peut alors effectuer un « produit en croix » et l'on obtient la multiplication $28 = 7 \times 4$. Que faire maintenant de 0 divisé par 7 ? Pour faciliter notre travail, appelons cette réponse a de sorte que

$$\frac{0}{7} = a$$

Avec un produit en croix, cela équivaut à $0 = 7 \times a$. Si c'est le cas, la seule valeur possible pour a est 0, car si la multiplication de deux nombres donne 0, alors l'un des deux doit être égal à 0.

Et ce n'est pas le plus difficile. Le point critique est la division par 0. Si l'on essaie de traiter 7/0 de la même manière que 0/7, on obtient l'équation

$$\frac{7}{0} = b$$

830 ap. J.-C.
Mahavira se penche sur les effets de l'introduction du zéro dans le système numérique.

1100
Bhaskara utilise 0 comme symbole en algèbre et entreprend de montrer comment il peut être utilisé.

1202
Fibonacci utilise le symbole supplémentaire 0 qu'il ajoute au système indo-arabe de chiffres de 1 à 9 mais ne lui donne pas le statut de nombre au même titre que les autres.

Avec le produit en croix, $0 \times b = 7$ et on aboutit à cette ineptie que $0 = 7$. Si l'on admet la possibilité pour 7/0 d'être un nombre, on risque alors une pagaille numérique à grande échelle. La solution est de dire que 7/0 est indéterminé. La division de 7 (ou de tout autre nombre que 0) par 0 ne débouche sur aucune réponse acceptable et c'est pourquoi cette opération n'est tout simplement pas autorisée. De manière similaire, il n'est pas permis de placer une virgule au « mi,lieu » d'un mot sans glisser dans l'absurde.

Le mathématicien indien Bhaskara au XIIe siècle, à la suite de Brahmagupta, n'écartait pas la division par 0 et suggérait qu'un nombre divisé par 0 était infini. Ce raisonnement se tient parce que si l'on divise un nombre par un très petit nombre, le résultat obtenu est très grand. Par exemple, 7 divisé par 1/10 est égal à 70 et 7 divisé par 1/100 donne 700. Plus on réduit le nombre du dénominateur, plus le nombre que l'on obtient est grand. Si l'on allait dans la petitesse ultime en prenant 0 lui-même, la réponse serait l'infini. En adoptant cette forme de raisonnement, nous nous trouvons obligés d'expliquer un concept plus bizarre encore, à savoir celui de l'infini. Se débattre avec l'infini n'aide pas ; l'infini (symbolisé aujourd'hui par ∞) ne suit pas les règles habituelles de l'arithmétique et n'est pas un nombre au sens habituel du terme.

Si 7/0 pose problème, que faire alors de l'encore plus bizarre 0/0 ? Si $0/0 = c$, avec le produit en croix on obtient l'équation $0 = 0 \times c$ et donc $0 = 0$. Cela n'apporte pas grand-chose, mais ce n'est pas absurde non plus. En fait, c peut être un nombre quelconque et ainsi, nous ne débouchons pas sur une impossibilité. Nous arrivons à la conclusion que 0/0 peut prendre n'importe quelle valeur, finie ou infinie ; les spécialistes parlent de « forme indéterminée ».

Pour résumer, l'étude de la division par zéro amène à la conclusion qu'il est préférable d'exclure cette opération de tous les calculs. L'arithmétique se porte tout aussi bien sans elle.

Pourquoi utiliser le zéro ? Il était tout simplement impossible de s'en passer. Les progrès de la science en dépendaient. On parle du degré zéro de longitude, du degré zéro sur l'échelle des températures et, de la même manière, de l'énergie du point zéro et du zéro absolu. Cette notion est entrée dans le langage courant avec des idées telles que le risque zéro et la tolérance zéro.

Une plus grande utilisation pourrait cependant en être faite. Si vous quittez la 5e avenue à New York et pénétrez dans l'Empire State Building, vous vous retrouvez dans le magnifique hall d'entrée au niveau 1. On utilise la capacité des nombres à s'ordonner, le 1 étant utilisé pour désigner le « premier » étage, le 2 pour désigner le « second » et ainsi de suite jusqu'à 102 pour le « cent deuxième » étage. En Europe, le rez-de-chaussée n'est en fait rien d'autre qu'un étage 0 que l'on a cependant quelques répugnances à appeler ainsi.

Les mathématiques ne pourraient pas fonctionner sans le zéro. C'est même un élément fondamental dans les concepts mathématiques qui régissent notre système

de nombres, l'algèbre et la géométrie. Sur la ligne des nombres, 0 est celui qui sépare les nombres positifs des nombres négatifs, et c'est pourquoi il occupe une position privilégiée. Dans le système décimal, le zéro sert de marqueur de position qui nous permet d'utiliser à la fois des nombres gigantesques et d'autres microscopiques.

Le zéro a mis des centaines d'années avant de se faire accepter et de devenir l'une des inventions les plus importantes de l'homme. Le mathématicien américain G. B. Halsted au XIXe siècle a détourné une réplique tirée du *Songe d'une nuit d'été* de Shakespeare pour dire que le zéro est le moteur du progrès qui « accorde à un rien dans l'air non seulement une demeure précise et un nom, une image, un symbole, mais également un pouvoir efficace ; il est la propriété du peuple indien qui lui a donné naissance. »

Au début, on a dû trouver le 0 tout à fait curieux, mais les mathématiciens ont la manie de s'enticher de concepts étranges qui s'avèrent utiles bien des années plus tard. C'est le cas aujourd'hui avec la théorie des ensembles où le concept d'un ensemble est défini comme une collection d'éléments. Dans cette théorie, Ø désigne l'ensemble qui ne contient aucun élément, ce que l'on désigne par « l'ensemble vide ». C'est un ensemble curieux, certes, mais comme 0, il est indispensable.

Tout sur rien

La somme de zéro et d'un entier strictement positif est strictement positive.
La somme de zéro et d'un entier strictement négatif est strictement négative.
La somme d'un entier strictement positif et d'un entier strictement négatif est égale à leur différence, ou, s'ils sont égaux, à zéro.
Zéro divisé par un entier strictement négatif ou positif est égal à zéro ou s'écrit sous la forme d'une fraction dont le numérateur est égal à zéro et le dénominateur est une quantité finie.

Brahmagupta, 628

idée clé
Rien est quelque chose

02 Les systèmes de nombres

Un système de nombres est un outil qui permet de traiter le concept de « quantité ». Diverses cultures à des moments différents de l'histoire ont adopté des méthodes variées, qui vont de la méthode de base « un, deux, trois, beaucoup » à la notation décimale hautement sophistiquée que nous utilisons aujourd'hui.

Les Sumériens et les Babyloniens, qui occupaient la Syrie, la Jordanie et l'Irak actuels il y a 4 000 ans environ, utilisaient un système de numérotation de position pour leur usage quotidien. Nous l'appelons système de position parce que l'on reconnaît le « nombre » grâce à la position d'un symbole. Ils utilisaient également 60 comme unité de base : c'est ce que nous appelons aujourd'hui un système sexagésimal ou système « en base 60 ». Il reste aujourd'hui des vestiges de la base 60. Il y a 60 secondes dans une minute, 60 minutes dans une heure. En ce qui concerne les angles, leur mesure repose aujourd'hui encore largement sur le système sexagésimal et s'exprime en degrés notés °. Ainsi, l'angle nul mesure 360° contre 400 grades avec le système décimal qui n'a jamais réussi à s'imposer. Un angle droit vaut donc 100 grades.

Nos très lointains ancêtres utilisaient principalement les nombres à des fins pratiques, et pourtant certains signes prouvent que les mathématiques en tant que telles excitaient la curiosité de ces cultures primitives, et qu'elles ont pris sur le temps réservé à l'exécution des tâches quotidiennes pour les explorer. Au nombre de ces explorations, figurent ce que l'on pourrait appeler « l'algèbre » et les propriétés des figures géométriques.

Le système égyptien du XIIIe siècle av. J.-C. utilisait la base 10 associée à un système de signes hiéroglyphiques. Les Égyptiens développèrent notamment un système destiné à traiter les fractions, mais la notation décimale de position actuelle nous est venue des Babyloniens, et ce sont les Indiens qui l'ont plus tard améliorée. Elle présente l'avantage de pouvoir exprimer à la fois de très petits nombres et de très gros. Les chiffres indo-arabes 1, 2, 3, 4, 5, 6, 7, 8 et 9 utilisés seuls permettent de

chronologie

300000 av. J.-C.
Les peuples européens du paléolithique comptent en faisant des entailles sur des os.

2000 av. J. C.
Les Babyloniens utilisent des symboles pour représenter les nombres.

calculer assez facilement. Pour le comprendre, examinons le système romain. Il était adapté à leurs besoins mais seuls des spécialistes du système étaient capables de s'en servir pour réaliser des calculs.

Le système romain Les symboles de base utilisés par les Romains étaient les « dix » (I, X, C et M), et leur moitié (V, L et D). Ces symboles sont combinés pour en former d'autres. On suppose que les symboles I, II, III et IIII tirent leur origine de l'apparence de nos doigts, V de la forme de notre main, et que, si l'on combine ce dernier symbole avec un V à l'envers de manière à former un X, on retrouve deux mains, ou dix doigts. C viendrait de *centum* et M de *mille*, mots latins signifiant respectivement cent et mille. Les Romains utilisaient aussi S pour « une moitié » ainsi qu'un système de fractions en base 12.

Le système romain utilisait une méthode qui reposait sur la position « avant et après » des symboles de base pour construire les combinaisons nécessaires, mais elle n'aurait, semble-t-il, pas été uniformément adoptée. Les Romains de l'Antiquité préféraient écrire IIII, alors que IV n'a été introduit que bien plus tard. La combinaison IX semble avoir été utilisée, mais pour un Romain,
SIX aurait signifié $8\frac{1}{2}$! Voici les nombres de base du système romain, avec quelques ajouts effectués à l'époque médiévale :

Le système de nombres romain

Empire Romain	**Extensions de l'époque médiévale**
S une moitié	
I un	
V cinq	$\overline{V}$ cinq mille
X dix	$\overline{X}$ dix mille
L cinquante	$\overline{L}$ cinquante mille
C cent	$\overline{C}$ cent mille
D cinq cents	$\overline{D}$ cinq cent mille
M mille	$\overline{M}$ un million

Il n'est pas facile de manier les chiffres romains. Il est par exemple impossible de comprendre MMMCDXLIIII si l'on n'introduit pas mentalement des parenthèses, de sorte que (MMM) (CD) (XL) (IIII) se lit alors 3 000 + 400 + 40 + 4 = 3 444. Mais essayez d'ajouter MMMCDXLIIII à CCCXCIIII. Un spécialiste romain de ce système aurait usé d'astuces pour s'en sortir, mais pour nous, il est difficile d'obtenir la bonne réponse sans d'abord effectuer le calcul dans le système décimal pour traduire ensuite le résultat en notation romaine :

Addition

	3 444	→	MMMCDXLIIII
+	394	→	CCCXCIIII
=	3 838	→	MMMDCCCXXXVIII

La multiplication de deux nombres est bien plus difficile et pourrait bien être impossible dans ce système de base, même pour les Romains ! Pour résoudre 3 444 × 394, il est nécessaire d'avoir recours aux extensions médiévales.

600 ap. J.-C.
L'ancêtre de notre numération décimale moderne est utilisée en Inde.

1200
Le système indo-arabe de notation des chiffres commence à se répandre.

1600
Les symboles du système décimal prennent les formes que nous leur connaissons aujourd'hui.

Multiplication

	3 444	→	MMMCDXLIIII
×	394	→	CCCXCIIII
=	1 356 936	→	$\overline{M}\overline{C}\overline{C}\overline{L}\overline{V}$MCMXXXVI

Les Romains n'avaient pas de symbole spécifique pour le zéro. Si vous aviez demandé à un citoyen végétarien de Rome de recenser le nombre de bouteilles de vin consommées dans sa journée, il aurait peut-être écrit III, mais si vous lui aviez demandé combien de poulets il avait mangé, il n'aurait pas pu écrire 0. Il reste des vestiges du système romain dans la pagination de certains livres (pas dans celui-ci cependant) et sur les frontons de certaines bâtisses. Certaines compositions n'ont jamais été utilisées par les Romains, comme MCM pour 1900 par exemple, mais elles ont été introduites à l'époque moderne pour satisfaire des préférences purement formelles. Les Romains auraient écrit MDCCCC. Le quatorzième Roi Louis de France, maintenant universellement connu sous le nom de Louis XIV, préférait en réalité se faire appeler Louis XIIII et avait décidé que le 4 des horloges devait s'écrire sous la forme IIII.



Pendule Louis XIIII

Représentation décimale des nombres entiers Dans le langage courant, on ne fait pas la différence entre « les nombres » et les nombres entiers. Le système décimal prend 10 pour base et utilise les chiffres 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9. Lorsque l'on écrit le nombre **394**, on peut expliciter sa signification décimale en disant qu'il est composé de 3 centaines, 9 dizaines et 4 unités, ce qui s'écrirait

$$\mathbf{394} = \mathbf{3} \times 100 + \mathbf{9} \times 10 + \mathbf{4} \times 1$$

On peut aussi l'écrire en utilisant des « puissances » de 10 (encore appelées « exposants ») :

$$\mathbf{394} = 3 \times 10^2 + \mathbf{9} \times 10^1 + \mathbf{4} \times 10^0$$

En effet $10^2 = 10 \times 10$, $10^1 = 10$ et nous admettons le cas à part $10^0 = 1$. Cette notation fait apparaître plus clairement la base décimale de notre système de nombres usuel, système grâce auquel l'addition et la multiplication gagnent en transparence.

La virgule décimale Jusque-là, nous avons examiné la représentation des nombres entiers. Le système décimal peut-il traiter des parties de nombre telles que $^{572}/_{1\,000}$? Cet exemple peut être noté sous la forme développée

$$\frac{572}{1000} = \frac{5}{10} + \frac{7}{100} + \frac{2}{1000}$$

On peut traiter les « réciproques » de 10, 100, 1 000 comme des puissances négatives de 10, de sorte que

$$\frac{572}{1000} = 5 \times 10^{-1} + 7 \times 10^{-2} + 2 \times 10^{-3}$$

ce qui peut s'écrire **0,572** avec une virgule qui indique le début des puissances négatives de 10. Si l'on ajoute ce résultat à la notation décimale de 394, on obtient l'expansion décimale du nombre $394^{572}/_{1\,000}$, c'est-à-dire **394,572** tout simplement.

Pour les très grands nombres, la notation décimale est parfois très longue, c'est pourquoi l'on revient dans ce cas à la « notation scientifique ». Par exemple, 1 356 936 892 peut s'écrire $1{,}356\,936\,892 \times 10^9$ qui apparaît souvent sous la forme « 1,356 936 892 × 10E9 » sur les calculatrices ou les ordinateurs. Dans cet exemple, la puissance 9 correspond au nombre de chiffres contenus dans le nombre moins 1 et la lettre E signifie « exposant ». Il nous arrive parfois de vouloir utiliser de plus grands nombres encore, par exemple pour parler du nombre d'atomes d'hydrogène que contient l'univers connu. On l'estime à environ $1{,}7 \times 10^{77}$. De la même manière, $1{,}7 \times 10^{-77}$, avec une puissance négative, est un très petit nombre qui est lui aussi facile à utiliser avec cette notation scientifique. On ne pourrait même pas imaginer ces nombres si l'on ne disposait que des symboles romains.

Les zéros et les uns Alors que la base 10 est parfaitement établie dans notre vie quotidienne, quelques applications nécessitent d'autres bases. Le système binaire qui utilise la base 2 se dissimule derrière notre puissant ordinateur moderne. La beauté de ce système réside dans le fait que l'on peut exprimer un nombre quel qu'il soit à l'aide des seuls symboles 0 et 1. En contrepartie de cette économie, les nombres écrits en base deux peuvent être très longs.

Comment écrire **394** en base 2 ? Cette fois, nous traitons de puissances de 2 et après quelques calculs, nous pouvons donner l'expression complète comme suit,

394 = **1** × 256 + **1** × 128 + **0** × 64 + **0** × 32 + **0** × 16 + 1 × 8 + **0** × 4 + 1 × 2 + **0** × 1

de sorte que, si on relève les zéros et les uns, **394** s'écrit **110001010** en base 2.

Comme les notations des nombres en base 2 peuvent être très longues, d'autres bases sont fréquemment utilisées en informatique. Il s'agit du système octal (base 8) et du système hexadécimal (base 16). Dans le système octal, seuls les symboles 0, 1, 2, 3, 4, 5, 6, 7, sont nécessaires, alors que le système hexadécimal utilise 16 symboles. Dans ce système en base 16, on utilise généralement 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Étant donné que 10 correspond à la lettre A, le nombre 394 s'écrit 18A en base hexadécimale. C'est l'ABC du système, ABC qui, dans le système décimal, équivaut à 2748, pensez-y !

Puissances de 2	Écriture décimale
2^0	1
2^1	2
2^2	4
2^3	8
2^4	16
2^5	32
2^6	64
2^7	128
2^8	256
2^9	512
2^{10}	1 024

l'idée clé
Notation des nombres

03 Les fractions

Une fraction est un « nombre fragmenté », au sens propre du terme. Pour fragmenter un nombre entier, la meilleure façon de procéder est d'utiliser des fractions. Prenons un exemple traditionnel, celui bien connu du gâteau que nous couperons ici en trois parts.

L'heureux convive qui reçoit deux des trois parts du gâteau en reçoit une fraction équivalente à 2/3. Son acolyte malheureux n'en reçoit que 1/3. En réunissant les deux portions du gâteau, on le reconstitue en entier, ou, sous forme de fractions, 1/3 + 2/3 = 1, où 1 représente le gâteau entier.

Voici un autre exemple. Imaginez que vous avez fait les soldes et que vous avez repéré une chemise affichée aux quatre cinquièmes de son prix initial. Dans ce cas, la fraction s'écrit 4/5. On pourrait également dire que la chemise est vendue un cinquième moins cher que son prix d'origine. On l'écrirait 1/5 et l'on voit alors que 1/5 + 4/5 = 1, 1 représentant le prix d'origine.

Une fraction prend toujours la forme d'un nombre entier placé « au-dessus » d'un autre nombre entier. Le nombre du bas s'appelle le « dénominateur » parce qu'il nous indique le nombre de parties égales qui constituent le tout. Le nombre du haut s'appelle le « numérateur » parce qu'il nous dit de combien de fractions unitaires est constituée cette partie du tout. Par conséquent, l'écriture d'une fraction se présente toujours comme suit

$$\frac{\textit{numérateur}}{\textit{dénominateur}}$$

Dans le cas du gâteau, la part que vous voulez peut-être manger correspond aux 2/3 du tout, et dans ce cas le dénominateur est égal à 3 et le numérateur à 2. La fraction 2/3 est constituée de 2 fractions unitaires égales à 1/3 chacune.

On peut aussi avoir des fractions telles que 14/5 (appelées fractions impropres) où le numérateur est plus grand que le dénominateur. Si l'on divise 14 par 5, on obtient 2 et il reste 4, ce qui peut s'écrire sous la forme du nombre « mixte » $2^{4}/_{5}$. Il est constitué du nombre entier 2 et de la fraction « propre » 4/5. Certains

chronologie

1800 av. J.-C.
Les fractions sont utilisées dans les cultures Babyloniennes.

1650 av. J.-C.
Les Égyptiens utilisent les fractions unitaires.

mathématiciens la notaient autrefois sous la forme $^{4}/_{5}2$. Les fractions sont généralement représentées avec un numérateur et un dénominateur (le « haut » et le « bas ») qui n'ont aucun facteur commun. Par exemple, le numérateur et le dénominateur de 8/10 ont 2 pour facteur commun, parce que $8 = 2 \times 4$ et $10 = 2 \times 5$. Si l'on écrit la fraction $8/10 = {}^{(2 \times 4)}/_{(2 \times 5)}$ on peut supprimer les 2 et donc 8/10 = 4/5, forme équivalente plus simple. Les mathématiciens appellent les fractions « des nombres rationnels » parce qu'elles expriment un ratio entre deux nombres. Les nombres rationnels étaient des nombres que les Grecs savaient « mesurer ».

Additionner et multiplier Chose curieuse avec les fractions, c'est qu'il est plus facile de les multiplier que de les additionner. La multiplication des nombres entiers est tellement pénible qu'il a fallu inventer des méthodes astucieuses pour y parvenir. Avec les fractions, c'est l'addition qui pose le plus de problèmes et qui demande un petit effort de réflexion.

Commençons par la multiplication. Si vous achetez une chemise aux quatre cinquièmes de son prix initial de 30 €, vous la payez au final 24 €. Les 30 € sont divisés en 5 parties de 6 € chacune et quatre de ces cinq parties sont égales à $4 \times 6 = 24$, somme à payer pour acheter la chemise.

Par la suite, le directeur du magasin découvre que ses chemises ne se vendent pas bien. Il baisse alors encore les prix et les affiche à $^{1}/_{2}$ du prix soldé. Si vous allez dans le magasin, vous pouvez maintenant acheter la chemise pour 12 €. On a en effet $^{1}/_{2} \times {}^{4}/_{5} \times 30$ qui est égal à 12 €. Pour multiplier deux fractions, il suffit de multiplier deux à deux les dénominateurs puis les numérateurs :

$$\frac{1}{2} \times \frac{4}{5} = \frac{1 \times 4}{2 \times 5} = \frac{4}{10}$$

Si le directeur avait fait les deux réductions en une seule fois, il aurait affiché les chemises à quatre dixièmes du prix initial qui est de 30 €, c'est-à-dire $^{4}/_{10} \times 30$, soit 12 €.

Additionner deux fractions est une tout autre affaire. L'addition de $^{1}/_{3} + {}^{2}/_{3}$ est simple parce que les dénominateurs sont identiques. Il suffit d'ajouter les deux numérateurs et l'on obtient $^{3}/_{3}$, ou 1. Mais comment additionner deux tiers du gâteau avec quatre cinquièmes du gâteau ? Comment calculer $^{2}/_{3} + {}^{4}/_{5}$? Si seulement on pouvait dire $^{2}/_{3} + {}^{4}/_{5} = {}^{(2+4)}/_{(3+5)} = {}^{6}/_{8}$, mais c'est malheureusement impossible.

Additionner les fractions exige une approche différente. Pour ajouter $^{2}/_{3}$ à $^{4}/_{5}$, il faut d'abord les mettre au même dénominateur. Commencez par multiplier le haut et le bas de $^{2}/_{3}$ par 5 : vous obtenez $^{10}/_{15}$. Multipliez à présent le haut et le bas de $^{4}/_{5}$ par 3 : vous obtenez $^{12}/_{15}$. Maintenant, les deux fractions ont 15 pour dénominateur commun et pour les additionner, il suffit d'additionner les numérateurs obtenus :

$$\frac{2}{3} + \frac{4}{5} = \frac{10}{15} + \frac{12}{15} = \frac{22}{15}$$

100 ap. J.-C.
Les Chinois conçoivent un système de calcul qui utilise des fractions.

1202
La notation fractionnaire avec la barre se répand grâce à Léonard de Pise (Fibonacci).

1585
Simon Stevin expose sa théorie sur les fractions décimales.

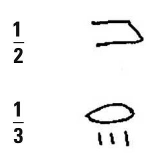
1700
Le trait de fraction « / » (comme dans $^{a}/_{b}$) est d'emploi courant.

Conversions sous forme décimale Dans le monde des sciences et dans la plupart des applications mathématiques, c'est sous forme décimale que l'on préfère exprimer les fractions. La fraction $^4/_5$ est équivalente à la fraction $^8/_{10}$ qui a 10 pour dénominateur et qui peut s'écrire sous la forme décimale 0,8.

Les fractions dont le dénominateur est égal à 5 ou 10 sont faciles à convertir. Mais comment pourrions-nous convertir par exemple $^7/_8$ sous forme décimale ? Tout ce qu'il faut savoir, c'est que lorsque l'on divise un nombre entier par un autre, ou bien il y va un certain nombre exact de fois, ou bien il y va un certain nombre de fois et il reste quelque chose que l'on appelle le « reste ».

Si l'on prend $^7/_8$ à titre d'exemple, la formule pour passer des fractions aux formes décimales est la suivante :

- Essayez de diviser 7 par 8. On ne peut pas, ou vous pourriez dire qu'il y va 0 fois et qu'il reste 7. On le note en écrivant zéro suivi de la virgule décimale : « 0, ».
- Maintenant, divisez 70 par 8 (le reste de l'étape précédente multiplié par 10). Il y va 8 fois, puisque $8 \times 8 = 64$; la réponse est donc 8 et il reste 6 (70 – 64). On écrit alors ce résultat à côté du précédent, ce qui donne « 0,8 ».
- Divisez à présent 60 par 8 (le reste de l'étape précédente multiplié par 10). Comme $7 \times 8 = 56$, la réponse est 7 et il reste 4. On le note, et nous en sommes maintenant à « 0,87 ».
- Divisez 40 par 8 (le reste de l'étape précédente multiplié par 10). Il y va 5 fois et il reste 0. Lorsque l'on obtient 0, on est arrivé au bout de la formule. C'est terminé. La réponse est « 0,875 ».



Avec d'autres fractions parfois, les choses ne s'arrêtent jamais ! On pourrait continuer à l'infini ; si l'on essaie de convertir $^2/_3$ sous forme décimale par exemple, on trouve que 20 divisé par 3 donne 6 et qu'il reste 2. Il faut alors diviser à nouveau 20 par 6, mais à aucun moment le reste n'est égal à 0. Dans ce cas, on obtient la forme décimale infinie 0,666666… On l'écrit 0,6–… pour indiquer que c'est une « fraction périodique ».

Un grand nombre de fractions nous mènent ainsi à l'infini. La fraction $^5/_7$ est intéressante. Dans ce cas, on a $^5/_7$ = 0,714 285 714 285 714 285… et on voit que la suite 714285 se répète périodiquement. Si une fraction quelconque donne une suite qui se répète périodiquement, il est impossible de l'écrire sous forme décimale et l'utilité de la notation avec la barre apparaît dans toute sa splendeur. Dans le cas de $^5/_7$ on écrit

$$\frac{5}{7} = 0,\overline{714\,285\ldots}$$



Fractions égyptiennes

Fractions égyptiennes Les Égyptiens du deuxième millénaire avant J.-C. avaient construit leur système de fractions à partir de hiéroglyphes qui désignaient des fractions unitaires, c'est-à-dire des fractions dont le numérateur est égal à 1. C'est ce que le papyrus Rhind entreposé au British Museum de Londres nous a enseigné. C'était un système de fractions si compliqué que

seuls ceux qui avaient reçu un enseignement spécifique en connaissaient tous les mystères pour réussir à effectuer parfaitement leurs calculs.

Les Égyptiens avaient une prédilection pour quelques fractions telles que $^2/_3$ mais toutes les autres fractions étaient exprimées sous forme de fractions unitaires, comme par exemple $^1/_2$, $^1/_3$, $^1/_{11}$ ou $^1/_{168}$. Ces « fractions de base » leur permettaient d'écrire toutes les autres fractions. Ainsi, $^5/_7$ n'est pas une fraction unitaire mais elle pourrait s'écrire en fractions unitaires sous la forme

$$\frac{5}{7} = \frac{1}{3} + \frac{1}{4} + \frac{1}{8} + \frac{1}{168}$$

Ici, il faut utiliser des fractions unitaires différentes. Une caractéristique du système est qu'il peut y avoir plusieurs écritures d'une même fraction, certaines étant plus courtes que d'autres. Par exemple

$$\frac{5}{7} = \frac{1}{2} + \frac{1}{7} + \frac{1}{14}$$

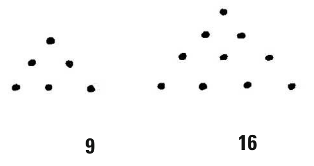
La « décomposition égyptienne » est peut-être d'une utilité pratique limitée mais le système a inspiré des générations de parfaits mathématiciens et fourni un grand nombre de problèmes stimulants, qui n'ont d'ailleurs pas tous été résolus aujourd'hui. Une analyse complète des méthodes qui permettraient de trouver la décomposition égyptienne la plus courte attend par exemple le vaillant explorateur des terres mathématiques.

l'idée clé
Un nombre placé au-dessus d'un autre

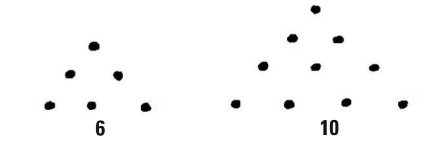
04 Les carrés et les racines carrées

Si vous aimez construire des carrés avec des points, alors vous avez l'esprit Pythagoricien. Cette activité était hautement prisée des membres de la Fraternité qui suivaient les principes imposés par leur maître Pythagore, personnage dont on se souvient davantage pour son célèbre théorème. Il naquit sur l'île grecque de Samos et fonda une société religieuse secrète qui prospéra en Italie du sud. Les disciples de Pythagore pensaient que les mathématiques étaient la clé pour comprendre l'essence de l'Univers.

Si l'on compte les points, on voit que le premier « carré » à gauche est constitué d'un seul point. Pour les Pythagoriciens, 1 était le nombre le plus important, car il était imprégné d'une existence toute spirituelle. C'est donc un bon début. Si l'on continue de compter les points dans les carrés suivants, on trouve les nombres « carrés » 1, 4, 9, 16, 25, 36, 49, 64… On les appelle les carrés « parfaits ». On peut calculer un carré parfait en additionnant le nombre total de points d'un carré donné au nombre de points situés sur deux côtés extérieurs du carré suivant, par exemple 9 + 7 = 16. Les disciples de Pythagore ne se sont pas arrêtés aux carrés. Ils se sont penchés sur d'autres figures, telles que le triangle, les pentagones (figures à cinq côtés) et autres figures polygonales (figures à plusieurs côtés).



Les nombres triangulaires ressemblent à un tas de pierres. Compter les points qui les constituent nous donne 1, 3, 6, 10, 15, 21, 28, 36, … Si vous voulez calculer un nombre triangulaire, il faut additionner le nombre de points d'un triangle donné au nombre de points de la dernière rangée du triangle suivant. Par exemple, quel nombre



chronologie

1750 av. J.-C.
Les Babyloniens établissent des tables de racines carrées.

525 av. J.-C.
Les Pythagoriciens étudient les carrés parfaits sous forme de points arrangés en figures géométriques.

Vers 300 av. J.-C.
La théorie d'Eudoxe sur les nombres irrationnels est publiée dans le livre 5 des *Éléments* d'Euclide.

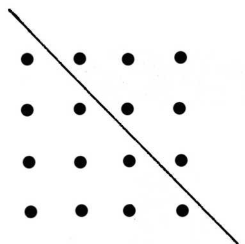
triangulaire vient après 10 ? Il aura 5 points sur sa dernière rangée et il suffit alors d'effectuer l'opération 10 + 5 = 15.

Si vous comparez les carrés parfaits aux nombres triangulaires, vous verrez que le nombre 36 apparaît dans les deux listes, mais il y a un lien bien plus surprenant encore entre ces nombres. Prenez des nombres triangulaires successifs et additionnez-les. Qu'obtenez-vous ? Essayons et notons les résultats obtenus dans un tableau.

Addition de deux nombres triangulaires successifs

1 + 3	4
3 + 6	9
6 + 10	16
10 + 15	25
15 + 21	36
21 + 28	49
28 + 36	64

C'est cela ! Lorsque vous additionnez deux nombres triangulaires successifs, vous obtenez un carré parfait. Vous pouvez aussi essayer avec une « preuve muette». Considérez un carré constitué de 4 rangées de 4 points traversé par une diagonale. Les points situés au-dessus de la diagonale (voir la figure) forment un nombre triangulaire, et en-dessous de cette diagonale se trouve le nombre triangulaire suivant. Cette observation est valable pour un carré de n'importe quelle taille. Avec ces « diagrammes à points », nous nous donnons les moyens de mesurer des aires. L'aire d'un carré dont le côté est 4 est $4 \times 4 = 4^2 = 16$ unités d'aire. En général, si l'on désigne le côté par x, alors l'aire sera égale à x^2.



La représentation graphique de la fonction x^2 est une courbe de forme parabolique qui correspond à la forme des antennes paraboliques de télévision ou des réflecteurs de phares de voiture. Une parabole possède un foyer. Un détecteur placé au foyer de la parabole concentre les signaux réfléchis lorsque des rayons parallèles provenant de l'espace viennent frapper l'antenne parabolique avant de converger vers le foyer.

Dans les phares de voiture, une ampoule placée en leur centre émet un rayon parallèle de lumière. En sport, les lanceurs de poids, de javelot et de marteau savent tous que la parabole est la trajectoire que décrit un objet en retombant à terre.

Les racines carrées Si l'on retourne la question et que l'on cherche la longueur du côté d'un carré dont l'aire est égale à 16, la réponse est tout simplement 4. La racine carrée de $\sqrt{16}$ est 4 et on l'écrit $\sqrt{16} = 4$. Le symbole $\sqrt{}$ est employé depuis les années 1500. Tous les carrés parfaits ont pour racines carrées de jolis nombres entiers. Par exemple, $\sqrt{1} = 1$, $\sqrt{4} = 2$, $\sqrt{9} = 3$, $\sqrt{16} = 4$, $\sqrt{25} = 5$, et ainsi de suite. Ces carrés parfaits ne se suivent cependant pas d'une traite sur la ligne des nombres. Viennent s'intercaler entre eux les nombres 2, 3, 5, 6, 7, 8, 10, 11…

630 ap. J.-C.
Brahmagupta donne des méthodes pour calculer les racines carrées.

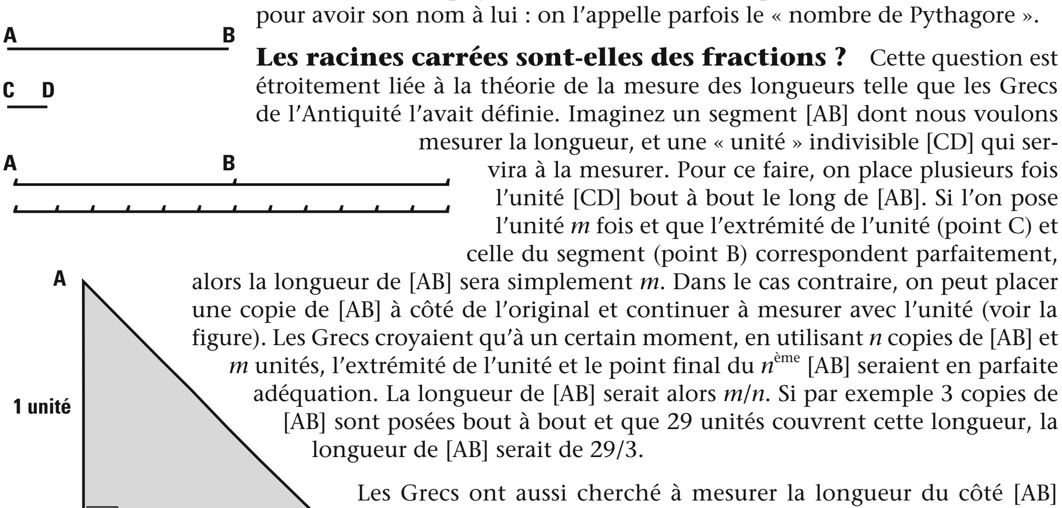
1550
Le symbole EF est introduit pour représenter les racines carrées.

1872
Richard Dedekind expose une théorie sur les nombres irrationnels.

Il existe une autre façon tout à fait admirable de noter les racines carrées. De même que x^2 indique un nombre élevé au carré, on peut écrire une racine carrée sous la forme $x^{1/2}$ qui concorde avec la formule selon laquelle on peut multiplier des nombres en additionnant leurs puissances. C'est la base des logarithmes inventés après que l'on eut compris aux alentours de 1600 comment on pouvait transformer un problème impliquant des multiplications en un problème d'additions. Mais c'est une autre histoire. Les nombres positifs ont tous des racines carrées qui ne sont pas nécessairement égales à des nombres entiers. Toutes les calculatrices sont virtuellement capables de donner la racine carrée d'un nombre grâce à la touche $\sqrt{\ }$. Si l'on tape $\sqrt{7}$ par exemple, elles affichent 2,645 751 311.

Examinons $\sqrt{2}$. Le nombre 2 avait une signification particulière pour les Pythagoriciens car c'est le premier nombre pair (pour les Grecs, les nombres pairs étaient féminins et les impairs masculins, tandis que les petits nombres avaient chacun une personnalité particulière). Si vous tapez $\sqrt{2}$ sur votre calculatrice, vous obtenez 1,414 213 562, en supposant que votre calculatrice vous donne autant de décimales. Est-ce donc la racine carrée de 2 ? Pour le vérifier, nous calculons 1,414 213 562 × 1,414 213 562. On obtient 1,999 999 999. Ce n'est pas tout à fait 2 car en fait 1,414 213 562 n'est qu'une approximation de la racine carrée de 2.

Ce qui est remarquable, c'est que nous ne réussirons jamais à obtenir autre chose qu'une valeur approchée de 2 ! On peut étendre l'écriture décimale de $\sqrt{2}$ à des millions de décimales, mais elle ne sera jamais rien d'autre qu'une approximation. Le nombre $\sqrt{2}$ est important en mathématiques. Bien sûr, il n'a peut-être pas tout l'éclat de π ou e (voir pages 20-27), mais il en a quand même suffisamment pour avoir son nom à lui : on l'appelle parfois le « nombre de Pythagore ».



Les racines carrées sont-elles des fractions ? Cette question est étroitement liée à la théorie de la mesure des longueurs telle que les Grecs de l'Antiquité l'avait définie. Imaginez un segment [AB] dont nous voulons mesurer la longueur, et une « unité » indivisible [CD] qui servira à la mesurer. Pour ce faire, on place plusieurs fois l'unité [CD] bout à bout le long de [AB]. Si l'on pose l'unité *m* fois et que l'extrémité de l'unité (point C) et celle du segment (point B) correspondent parfaitement, alors la longueur de [AB] sera simplement *m*. Dans le cas contraire, on peut placer une copie de [AB] à côté de l'original et continuer à mesurer avec l'unité (voir la figure). Les Grecs croyaient qu'à un certain moment, en utilisant *n* copies de [AB] et *m* unités, l'extrémité de l'unité et le point final du $n^{\text{ème}}$ [AB] seraient en parfaite adéquation. La longueur de [AB] serait alors m/n. Si par exemple 3 copies de [AB] sont posées bout à bout et que 29 unités couvrent cette longueur, la longueur de [AB] serait de 29/3.

Les Grecs ont aussi cherché à mesurer la longueur du côté [AB] (l'hypoténuse) d'un triangle dont les deux autres côtés ont une longueur d'« unité » 1. Selon le théorème de Pythagore, la

longueur de [AB] pourrait s'écrire symboliquement sous la forme $\sqrt{2}$; la question est donc de savoir si $\sqrt{2} = m/n$.

Avec notre calculatrice, nous avons déjà vu que l'expression décimale de $\sqrt{2}$ est potentiellement infinie, ce qui indique peut-être que $\sqrt{2}$ n'est pas une fraction. Toutefois, le rationnel 0,3333333… n'a pas de fin et pourtant, il représente la fraction $^1/3$. Il nous faut des arguments plus convaincants.

Est-ce que $\sqrt{2}$ est une fraction ? Cette question débouche sur l'une des preuves les plus célèbres des mathématiques. Elle se situe dans la lignée de ce type de preuves dont les Grecs étaient friands : la méthode de raisonnement par l'absurde. On a d'abord abordé ce problème en disant que $\sqrt{2}$ ne peut pas à la fois être une fraction et ne pas en être une. C'est ce que l'on appelle en logique la loi du « tiers exclu ». Mais cette logique n'autorise pas de solution intermédiaire. La méthode suivie par les Grecs était donc astucieuse. Ils ont admis que c'était une fraction et, selon une logique parfaitement rigoureuse appliquée à chaque étape du raisonnement, ils en ont tiré une contradiction, une « absurdité ». Suivons donc ce raisonnement. Supposez que

$$\sqrt{2} = \frac{m}{n}$$

On peut allez un peu plus loin. On peut supposer que m et n n'ont aucun facteur commun. C'est correct car s'ils en avaient, on pourrait les éliminer avant de commencer. (Par exemple, la fraction 21/35 est égale à la fraction 3/5 après élimination du facteur commun 7.)

On peut élever au carré les deux côtés de $\sqrt{2} = m/n$ pour obtenir $2 = m^2/n^2$ et donc $m^2 = 2n^2$. C'est ici que l'on peut faire la première observation : puisque m^2 est le double d'un entier, ce doit être un nombre pair. Ensuite, m lui-même ne peut pas être impair (parce que le carré d'un nombre impair est impair) et donc m est aussi un nombre pair.

Jusque-là, la logique est impeccable. Comme m est pair, il doit être égal au double d'un entier que l'on peut écrire sous la forme $m = 2k$. Élever au carré les deux côtés signifie que $m^2 = 4k^2$. Or, $m^2 = 2n^2$, donc $2n^2 = 4k^2$ et en simplifiant par 2, on peut conclure que $n^2 = 2k^2$. C'est du déjà vu ! Et comme précédemment, on conclut que n^2 est pair et que n lui-même est pair. En suivant une logique rigoureuse, nous en avons déduit que m et n sont tous deux pairs et qu'ils ont donc comme facteur commun 2. Ce résultat est contraire à notre supposition de départ que m et n n'ont pas de facteurs communs. La conclusion est donc que $\sqrt{2}$ ne peut pas être une fraction.

On peut aussi prouver que toute la suite de nombres $\sqrt{n}$ (sauf lorsque n est un carré parfait) ne peuvent pas être des fractions. Les nombres qui ne peuvent pas être exprimés sous forme de fractions sont appelés les nombres « irrationnels », et nous avons donc observé qu'il y a un nombre infini de nombres irrationnels.

l'idée clé
Vers les nombres irrationnels

05 π

π est le nombre le plus célèbre des mathématiques. Oubliez toutes les autres constantes de la Nature, π sera toujours en tête de liste. S'il y avait des Oscars pour les nombres, π serait récompensé chaque année.

π, ou pi, est égal à la longueur d'un cercle (sa circonférence) divisée par la longueur du segment qui passe par son centre (son diamètre). Sa valeur, le rapport entre ces deux longueurs, ne dépend pas de la taille du cercle. Que le cercle soit grand ou petit, π est en effet une constante mathématique. Le cercle est le cadre naturel de π mais on le rencontre partout en mathématiques, et à des endroits qui n'ont rien à voir avec les cercles.

Archimède de Syracuse Le rapport entre la circonférence d'un cercle et son diamètre est un sujet qui intéresse les mathématiciens depuis longtemps. Vers 2000 av. J.-C., les Babyloniens ont observé que la circonférence d'un cercle était environ trois fois plus grande que son diamètre.

C'est Archimède de Syracuse qui est à l'origine des premières découvertes mathématiques sur π, aux alentours de 225 av. J.-C. Archimède figure parmi les plus grands. Les mathématiciens aiment évaluer leurs collègues et ils le placent au même niveau que Carl Friedrich Gauss (Le « Prince des Mathématiciens ») et que Sir Isaac Newton. Quels que soient les mérites de ce jugement, il est clair qu'Archimède se trouverait dans n'importe quel panthéon dédié aux mathématiques. Il n'était certainement pas homme à vivre enfermé dans sa tour d'ivoire, car en plus de ses contributions à l'astronomie, aux mathématiques et à la physique, il conçut également des armes de guerre telles que des catapultes, des leviers et des « miroirs brûlants », armes qui avaient toutes leur utilité pour maintenir les Romains à distance. Il avait toutefois quelque chose du professeur distrait, car sinon, pourquoi se serait-il précipité hors de son bain pour s'élancer tout nu dans la rue en s'écriant « Eurêka » alors qu'il venait de découvrir la loi de la poussée qui porte son nom ? On ignore de quelle manière il a fêté ses découvertes sur π.

Pour un cercle de diamètre *d* et de rayon *r* :
Circonférence = $\pi d = 2\pi r$
Aire = πr^2
Pour une sphère de diamètre *d* et de rayon *r* :
Surface = $\pi d^2 = 4\pi r^2$
Volume = $\frac{4}{3}\pi r^3$

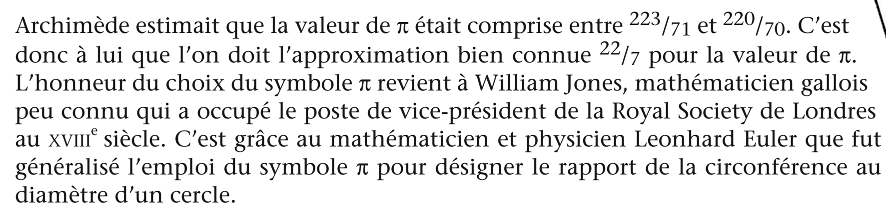
chronologie

2000 av. J.-C.
Les Babyloniens observent que π est à peu près égal à 3.

250 av. J.-C.
Archimède donne une valeur approchée de π égale à 22/7.

Puisque π est défini comme le rapport entre la circonférence et le diamètre d'un cercle, quel est le lien entre π et l'aire d'un cercle ? Par déduction, on sait que l'aire d'un cercle de rayon r est πr^2, mais on connaît probablement moins bien la définition de π comme rapport entre la circonférence et le diamètre d'un cercle. La double fonction de π, qui sert à la fois pour calculer l'aire et la circonférence, est remarquable.

Comment le démontrer ? Le cercle peut être divisé en plusieurs triangles égaux de base b et dont la hauteur est à peu près égale au rayon r. Ils constituent un polygone à l'intérieur du cercle qui correspond approximativement à l'aire du cercle. Prenons 1 000 triangles pour commencer. Il s'agit en fait d'un exercice d'approximations. On peut réunir chaque paire adjacente de ces triangles pour former un rectangle (à quelque chose près) d'aire $b \times r$ de sorte que l'aire totale du polygone sera de $500 \times b \times r$. Comme $500 \times b$ correspond à peu près à la moitié de la circonférence, il a pour longueur πr, et donc l'aire du polygone est $\pi r \times r = \pi r^2$. Plus il y a de triangles, meilleure est l'approximation et, en tendant vers l'infini, on en déduit que l'aire du cercle est πr^2.



Archimède estimait que la valeur de π était comprise entre $^{223}/_{71}$ et $^{220}/_{70}$. C'est donc à lui que l'on doit l'approximation bien connue $^{22}/_{7}$ pour la valeur de π. L'honneur du choix du symbole π revient à William Jones, mathématicien gallois peu connu qui a occupé le poste de vice-président de la Royal Society de Londres au XVIIIe siècle. C'est grâce au mathématicien et physicien Leonhard Euler que fut généralisé l'emploi du symbole π pour désigner le rapport de la circonférence au diamètre d'un cercle.

La valeur exacte de π Il est absolument impossible de connaître la valeur exacte de π car c'est un nombre irrationnel. C'est ce que Johann Lambert a démontré en 1768. Son développement décimal est infini et imprévisible. Les 20 premières décimales sont 3,14159265358979323846… La valeur $\sqrt{10}$ utilisée par les mathématiciens chinois et adoptée aux alentours de 500 par Brahmagupta est égale à 3,16227766016837933199. Cette valeur est un peu meilleure que la valeur grossière 3 et diffère de celle de π au niveau de la seconde décimale.

On peut calculer π à partir d'une série de nombres. On connaît la série

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \ldots$$

dont la convergence sur π est affreusement lente cependant et épouvantable à calculer. Euler a découvert une série tout à fait remarquable qui converge vers π :

$$\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \ldots$$

1706 ap. J.-C.
William Jones introduit le symbole π.

1761
Lambert prouve l'irrationalité de π.

1882
Lindemann prouve la transcendance de π.

Srinivasa Ramanujan, autodidacte de génie, est à l'origine de formules spectaculaires qui convergent vers π. En voici une qui repose uniquement sur la racine carrée de 2 :

$$\frac{9801}{4412}\sqrt{2} = 3{,}141592\underline{7}300133056603139961890\ldots$$

Les mathématiciens sont fascinés par π. Alors que Lambert avait prouvé qu'il ne pouvait pas être un nombre rationnel, le mathématicien allemand Ferdinand von Lindemann a trouvé en 1882 la solution au problème le plus coriace concernant π. Il a prouvé que π était « transcendant », c'est-à-dire qu'il ne pouvait être solution d'aucune équation algébrique à coefficients entiers (une équation avec des puissances entières de x uniquement). En trouvant la clé de cette « énigme ancestrale», Lindemann a résolu le problème de la « quadrature du cercle ». Étant donné un cercle, le défi était de construire un carré d'une aire identique à la règle et au compas seulement. Lindemann a définitivement prouvé que c'était impossible. De nos jours, l'expression « c'est la quadrature du cercle » est devenue synonyme d'une impossibilité.

Le calcul de la valeur de π a rapidement progressé. En 1873, William Shanks a déterminé la valeur exacte des 707 premières décimales de π (elles sont en fait correctes jusqu'à la 527e décimale). Au XXe siècle, la quête pour calculer le plus grand nombre de décimales de π s'est accélérée grâce à l'ordinateur. En 1949, on est allé jusqu'à 2 037 décimales de π, ce qui nécessita 70 heures de travail sur un ordinateur ENIAC. Dès 2002, on a atteint le nombre stupéfiant de 1 241 100 000 000 décimales, mais ce n'est sûrement pas fini. Si nous étions au niveau de l'équateur, et si nous voulions recopier le développement décimal de π, le calcul de Shanks s'étalerait sur 14 mètres mais le résultat obtenu en 2002 nous ferait faire 62 tours du monde !

On s'est posé de nombreuses questions sur π qui ont pour beaucoup reçu une réponse. Les décimales de π sont-elles aléatoires ? Est-il possible de trouver une suite donnée dans le développement décimal de π ? Par exemple, est-il possible de trouver la suite 0123456789 ? Dans les années 1950, on croyait que cela appartenait au domaine de l'inconnaissable. Personne n'avait trouvé une telle suite dans les 2 000 premières décimales de π. L.E.J. Brouwer, mathématicien hollandais de renom, affirma même que ce genre de problème était dénué de sens car il était selon lui empiriquement impossible à vérifier. En fait, une suite de chiffres fut trouvée en 1997 au niveau de la 17 387 594 880e décimale, ou, pour utiliser la métaphore de l'équateur, environ 5 000 kilomètres avant la fin d'un tour du monde complet. Vous trouverez le chiffre 6 dix fois de suite avant d'avoir fait 1 000 kilomètres mais il vous faudra attendre la fin d'un tour complet et parcourir encore presque 6 000 kilomètres avant de trouver le chiffre 7 dix fois de suite.

L'importance de π À quoi cela sert-il de connaître tant de décimales de π ? Après tout, la plupart des calculs impliquant π ne nécessitent que quelques décimales ; il n'en faut probablement pas plus de dix quelle que soit l'application pratique concernée, et l'approximation d'Archimède de 22/7 est la plupart du temps suffisante. Toutefois, les calculs du développement décimal de π ne sont pas

seulement effectués pour le plaisir. Ils permettent de tester le bon fonctionnement des ordinateurs, en plus d'exercer une fascination sur un groupe de mathématiciens qui se sont baptisés eux-mêmes les « amis de pi ».

L'épisode le plus étrange dans l'histoire de π fut peut-être la tentative de l'assemblée législative de l'État de l'Indiana aux États-Unis de faire passer une loi pour fixer la valeur de π. C'est à la fin du XIXe siècle qu'un médecin, le docteur E. J. Goodwin, a déposé le projet de loi pour rendre π « plus digeste ». Le problème est que l'auteur de la proposition fut incapable de fixer la valeur de π. Heureusement pour l'Indiana, on s'est rendu compte que c'était pure folie de vouloir légiférer sur la valeur de π. Depuis lors, les hommes politiques laissent π tranquille.

π en poésie

Si vous tenez à mémoriser les premiers chiffres du développement de π, un peu de poésie pourrait vous aider. Parmi les procédés mnémotechniques traditionnellement utilisés dans l'enseignement des mathématiques, figure une variante remarquable du poème « The Raven » d'Edgar Alan Poe, variante que l'on doit à Michael Keith.

Le poème original de Poe commence ainsi	**La variante de Keith pour π commence ainsi**
The raven, E.A. Poe	Poe, E. *Near A Raven*
Once upon a midnight dreary, while I pondered weak and weary,	*Midnights so dreary, tired and weary.*
Over many a quaint and curious volume of forgotten lore,	*Silently pondering volumes extolling all by-now obsolete lore.*

Le nombre de lettres contenues dans chaque mot successif de la version de Keith donne les 740 premières décimales de π[1].

1. En français, il existe des textes du même genre qui permettent de mémoriser π. L'un d'eux commence ainsi : « Que j'aime à faire connaître un nombre utile aux sages ! Glorieux Archimède, artiste ingénieux, Toi de qui Syracuse aime encore la gloire, Soit ton nom conservé par de savants grimoires ! … ». (NdT)

l'idée clé
Lorsque la valeur de π était ouverte

06 *e*

***e* fait figure de novice à côté de π, son unique rival. Alors que, tout auréolé de son passé magnifique qui remonte aux Babyloniens, π le domine par l'éclat de sa grandeur, *e* est beaucoup moins accablé par le poids de l'histoire. La constante *e*, toute vibrante de jeunesse, est toujours là quand il s'agit de « croissance ». Que l'on s'intéresse aux populations, à l'argent ou à d'autres quantités physiques, la croissance implique invariablement la présence de *e*.**

e est le nombre dont la valeur est à peu près égale à 2,71828. Mais alors, qu'a-t-il donc de si particulier ? Ce n'est pas un nombre pris au hasard, mais l'une des grandes constantes mathématiques. Elle fut découverte au début du XVII[e] siècle lorsque plusieurs mathématiciens ont consacré tout leur temps à mettre au point l'idée d'un logarithme, superbe invention qui a permis de substituer une addition à une multiplication entre de très grands nombres.

Tout a commencé avec une histoire d'argent. Jacob Bernoulli appartenait à cette illustre famille Suisse qui avait fournit une dynastie de mathématiciens au monde entier. Jacob commença ses recherches sur le problème des intérêts composés en 1683.

Gros sous Prenons une période de 1 an, un taux d'intérêt faramineux de 100 % et un versement initial (appelé « capital ») de 1 €. Il est bien sûr très rare d'obtenir un taux d'intérêt aussi élevé, mais ce chiffre nous convient car le concept peut ainsi être facilement adapté à des taux d'intérêt réalistes tels que 6 % ou 7 %. De même, si nous plaçons des sommes plus importantes, 10 000 € par exemple, il suffit de multiplier le tout par 10 000.

Avec un intérêt de 100 %, nous percevrons à la fin de l'année notre capital auquel s'ajouteront des intérêts qui, dans ce cas, seront de 1 €. Nous percevrons donc la magnifique somme de 2 €. Supposons maintenant que le taux d'intérêt soit réduit de moitié mais qu'il s'applique tous les six mois pendant un an. À la fin des six premiers mois, nous touchons 50 centimes d'intérêts et notre capital s'élève maintenant à 1,50 €. À la fin de la première année, nous touchons donc cette somme plus les 75 centimes d'intérêts qu'elle à générés. Nous sommes passés de 1 € à 2,25 € à la fin de l'année ! Avec ce système d'intérêts composés tous les six mois, nous

chronologie

1618
Les travaux de John Neper sur les logarithmes font apparaître une nouvelle constante, *e*.

1727
Euler utilise la notation *e* dans son travail sur la théorie des logarithmes ; on l'appelle parfois le nombre d'Euler.

gagnons 25 centimes de plus. À première vue, ce n'est peut-être pas beaucoup, mais si nous avions un capital de10 000 €, nous toucherions 2 250 € d'intérêts au lieu de 2 000 €. Ce système permet de percevoir 250 € de plus.

Cependant, si choisir un intérêt composé sur six mois signifie que nous augmentons notre capital, la banque augmente le sien si nous lui devons de l'argent : alors prudence ! Supposons maintenant que l'année est divisée en quatre, et qu'un taux de 25 % s'applique sur chacune des quatre périodes. En effectuant un calcul similaire, on trouve que notre 1 € grossit pour atteindre 2,44141 €. Notre capital augmente et avec nos 10 000 €, il semblerait avantageux de découper l'année en périodes plus courtes et de leur appliquer des taux d'intérêts plus bas.

Notre argent augmentera-t-il à l'infini et deviendrons-nous millionnaires ? Si nous continuons à diviser l'année en unités de plus en plus petites, comme dans le tableau, ce « processus restrictif » montre que la somme totale semble se stabiliser vers un nombre constant. Bien sûr, la seule période réaliste de capitalisation des intérêts est le jour (c'est la période choisie par les banques). Le message mathématique est que la limite, que les mathématiciens appellent *e*, est égale à la somme générée par 1 € si la capitalisation des intérêts se produit en continu. Est-ce une bonne ou une mauvaise chose ? Vous connaissez la réponse : si vous économisez, « oui » ; si vous devez de l'argent, « non ». C'est un problème « d'*e*… xpert».

Intérêts composés par accroissement du capital	
An	2,00000 £
Six mois	2,25000 £
Trimestre	2,44141 £
Mois	2,61304 £
Semaine	2,69260 £
Jour	2,71457 £
Heure	2,71813 £
Minute	2,71828 £
Seconde	2,71828 £

La valeur exacte de *e* Comme π, *e* est un nombre irrationnel et comme π, sa valeur exacte ne peut donc pas être connue. La valeur approchée de *e* est 2,71828182845904523536… si l'on s'arrête aux 20 premières décimales.

Exprimée sous forme de fractions, la meilleure approximation de la valeur de *e* est 87/32 si l'on se limite à des nombres à deux chiffres pour le numérateur et le dénominateur. Curieusement, si l'on choisit des nombres à trois chiffres, la meilleure fraction est 878/323. C'est une sorte de développement palindromique de la première : les mathématiques nous offrent parfois ce genre de petites surprises. Voici un développement de suite bien connu pour *e* :

$$e = 1 + \frac{1}{1} + \frac{1}{1\times 2} + \frac{1}{1\times 2\times 3} + \frac{1}{1\times 2\times 3\times 4} + \frac{1}{1\times 2\times 3\times 4\times 5} + \ldots$$

1748
Euler calcule 23 décimales de *e* ; on lui attribue la découverte de la célèbre formule $e^{i\pi} + 1 = 0$ aux alentours de cette période.

1873
Hermite prouve que *e* est un nombre transcendant.

2007
On connaît jusqu'à 10^{11} décimales de *e*.

La notation factorielle qui utilise le point d'exclamation est ici commode. On peut écrire, par exemple, $5! = 1 \times 2 \times 3 \times 4 \times 5$. En utilisant cette notation, e s'écrit sous la forme plus connue :

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!} + \ldots$$

Le nombre e semble donc bien avoir une structure. Il paraît plus « symétrique » que π au niveau de ses propriétés mathématiques.

Si vous voulez une technique pour mémoriser les premières décimales de e, essayez ceci : « We attempt a mnemonic to remember a strategy to memorize this count… », où le nombre de lettres de chaque mot donne une décimale de e. Si vous avez quelques notions d'histoire américaine, vous pouvez vous souvenir que e, c'est « 2,7 Andrew Jackson Andrew Jackson », parce que Andrew Jackson (surnommé « Old Hickory »), le septième président des États-Unis, a été élu en 1828. Il existe bien d'autres techniques pour se souvenir de e, mais leur intérêt réside davantage dans leur bizarrerie que dans leur valeur mathématique.

Le fait que e est irrationnel (il ne peut pas s'écrire sous forme de fraction) a été prouvé par Leonhard Euler en 1737. En 1840, le mathématicien français Joseph Louisville a démontré que e n'était la solution d'aucune équation de degré deux à coefficients entiers, et en 1873, par un travail novateur, son compatriote Charles Hermite a prouvé la transcendance de e (il n'est la solution d'aucune équation algébrique à coefficients entiers). La méthode, plus que le résultat, était cruciale. Neuf ans plus tard, Ferdinand von Lindemann utilisa cette même méthode pour prouver que π était transcendant, ce qui avait plus de cachet.

On avait résolu un problème mais d'autres surgirent. Si on élève e à la puissance e, est-il transcendant ? Quelle question bizarre, comment pourrait-il en être autrement ? Personne cependant n'en a apporté une preuve rigoureuse et, si l'on s'en tient à des critères mathématiques purs, cette question reste une conjecture. Certains mathématiciens ont fait de petites avancées en démontrant qu'il est impossible que e et e^{e2} soient tous les deux transcendants. Bien joué, mais ce n'est pas encore ça.

Les liens entre π et e sont fascinants. Les valeurs de e^{π} et π^{e} sont proches mais on montre facilement (sans calculer leurs valeurs) que $e^{\pi} > \pi^{e}$. Si vous « trichez » et jetez un œil sur votre calculatrice, vous verrez qu'elle donne les valeurs approchées suivantes : $e^{\pi} = 23{,}14069$ et $\pi^{e} = 22{,}45916$.

Le nombre e^{π} est connu sous le nom de constante de Gelfond (d'après le nom du mathématicien russe Aleksandr Gelfond) et sa transcendance a été montrée. On en sait beaucoup moins sur π^{e}. Personne n'a encore prouvé qu'il était irrationnel, mais l'est-il vraiment ?

***e* est-il important ?** On rencontre principalement e dans les problèmes de croissance. On pense par exemple à la croissance économique et à la croissance des populations. On trouve également e dans certaines fonctions exponentielles qui modélisent la désintégration radioactive.

Le nombre *e* apparaît aussi dans des problèmes qui n'ont rien à voir avec la croissance. Au XVIII[e] siècle, Pierre Montmort examina un problème de probabilités que l'on a amplement étudié depuis. Dans sa version simple, un groupe de personnes vont manger ensemble et reprennent leur chapeau au hasard à la fin du repas. Quelle est la probabilité pour que personne ne retrouve son chapeau ?

On peut montrer que cette probabilité est de $^1/_e$ (environ 37 %) de sorte que la probabilité pour qu'une personne au moins retrouve son chapeau est de $1 - {}^1/_e$ (63 %). C'est une application parmi d'autres, très nombreuses, de la théorie des probabilités. La loi de Poisson, loi qui traite des événements rares, en est une autre. Ces premiers exemples n'étaient en aucun cas isolés : James Stirling réussit une approximation remarquable de la valeur factorielle de $n!$ en utilisant *e* (et π) ; en statistique, la « courbe en cloche » appelée courbe de Gauss de la distribution normale a recours à *e* ; et en mécanique, la courbe que suit un câble de pont suspendu se calcule avec *e*. La liste est infinie.

La loi normale

Une identité stupéfiante La formule la plus remarquable de toutes les mathématiques contient *e*. Lorsque l'on pense aux nombres célèbres des mathématiques, on pense à 0,1, π, *e* et au nombre imaginaire $i = \sqrt{-1}$. Comment se pourrait-il que

$$e^{i\pi} + 1 = 0$$

C'est possible ! C'est un résultat que l'on attribue à Euler.

L'importance réelle de *e* tient peut-être au mystère qui l'entoure et qui a captivé des générations de mathématiciens. Pour tout dire, *e* est incontournable. Sinon, pourquoi un auteur tel que Georges Pérec se serait-il lui-même mis au défi d'écrire un roman où la lettre « e » n'apparaît jamais ? C'est l'unique raison d'être de son roman *La Disparition*. On imagine difficilement qu'un mathématicien puisse se mettre en tête d'écrire un manuel qui ne contiendrait pas *e*, et qu'il y parvienne de surcroît.

l'idée clé
Le plus naturel des nombres

07 L'infini

Quelle est la taille de l'infini ? Pour faire court, on dit que ∞ (le symbole pour représenter l'infini) est très grand. Pensez à une droite sur laquelle se succèdent des nombres de plus en plus grands et ce « jusqu'à l'infini ». Chaque nombre très grand, comme $10^{1\,000}$, est toujours suivi d'un nombre encore plus grand, par exemple $10^{1\,000} + 1$.

C'est ainsi que l'on se représente habituellement l'infini, avec des nombres qui augmentent sans cesse. Les mathématiques utilisent l'infini dans tous les domaines, mais il faut faire attention lorsque l'on traite l'infini comme un nombre ordinaire. Ce n'en est pas un.

Compter Le mathématicien allemand Georg Cantor nous a légué un concept de l'infini entièrement nouveau. Ce faisant, il a créé à lui seul une théorie qui a influencé une grande partie des mathématiques modernes. L'idée sur laquelle repose la théorie de Cantor est liée à une technique rudimentaire utilisée pour compter, plus simple encore que celle que l'on utilise dans nos activités quotidiennes.

Imaginez un fermier qui ne sait pas compter avec des nombres. Comment pourrait-il savoir combien il possède de moutons ? C'est simple : quand il les fait sortir le matin, il peut savoir s'ils sont tous de retour le soir s'il associe à chaque mouton une pierre prise dans un tas placé à l'entrée de son champ. S'il manque un mouton, il restera une pierre. Sans même utiliser de nombre, notre fermier a vraiment le sens des mathématiques. Il utilise l'idée d'une correspondance bijective entre les moutons et les pierres. Cette idée de base a eu quelques conséquences surprenantes.

La théorie de Cantor fait appel à des ensembles (un ensemble est une collection d'objets). Par exemple, **N** = {0,1, 2, 3, 4, 5, 6, 7, 8…} désigne l'ensemble de tous les entiers naturels. Une fois qu'un ensemble est défini, on peut parler de sous-ensembles, c'est-à-dire d'ensembles contenus dans le premier. Les sous-ensembles les plus évidents associés à notre exemple **N** sont les sous-ensembles **I** = {1, 3, 5, 7…} et **P** = {0, 2, 4, 6, 8…}, qui sont respectivement les ensembles des nombres impairs et des nombres pairs. À la question : « Y a-t-il autant de nombres impairs que de nombres pairs ? », quelle serait notre réponse ? Impossible de compter les éléments de chaque ensemble et de les comparer, et pourtant, notre réponse

chronologie

350 av. J.-C.
Aristote rejette l'idée d'un infini réel.

1639 ap. J.-C.
Girard Desargues introduit le concept d'infini en géométrie.

serait certainement « oui, absolument ». Mais sur quoi repose cette certitude ? Probablement sur une idée du genre « la moitié de tous les nombres sont impairs et la moitié sont pairs ». Cantor serait d'accord avec nous mais son explication serait différente. Il dirait que tout nombre impair est suivi d'un « partenaire » pair. L'idée que les deux ensembles **I** et **P** ont le même nombre d'éléments repose sur l'idée que tout nombre impair peut être associé à un nombre pair :

I :	1	3	5	7	9	11	13	15	17	19	21
	•	•	•	•	•	•	•	•	•	•	•
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	•	•	•	•	•	•	•	•	•	•	•
P :	0	2	4	6	8	10	12	14	16	18	20

À cette autre question : « Y a-t-il le même nombre de nombres entiers que de nombres pairs ? » la réponse serait peut-être « non », l'argument étant que l'ensemble **N** contient deux fois plus de nombres que celui des nombres pairs.

La notion de « plus », cependant, est plutôt floue lorsqu'il s'agit d'ensembles qui contiennent un nombre infini d'éléments. Nous pourrions mieux faire en utilisant l'idée d'une correspondance bijective. Et bizarrement, il y a une bijection entre **N** et l'ensemble des nombres pairs **P** :

N :	0	1	2	3	4	5	6	7	8	9	10	11
	•	•	•	•	•	•	•	•	•	•	•	•
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
	•	•	•	•	•	•	•	•	•	•	•	•
P :	0	2	4	6	8	10	12	14	16	18	20	22

Nous arrivons à cette conclusion stupéfiante qu'il y a le « même nombre » de nombres entiers que de nombres pairs ! C'est un défi à la « notion commune » formulée par les Grecs de l'Antiquité : Euclide d'Alexandrie, au début de ses *Éléments*, dit que « le tout est plus grand que la partie ».

Cardinal Le nombre d'éléments d'un ensemble fini E s'appelle le « cardinal » de E. Par exemple, le cardinal de l'ensemble des moutons du fermier est égal à 42. Le cardinal de l'ensemble $\{a, b, c, d, e\}$ est égal à 5 et se note Card $\{a, b, c, d, e\} = 5$. Le cardinal est donc la mesure de la « taille » d'un ensemble. Pour exprimer le cardinal de l'ensemble **N**, et de tout ensemble dont les éléments sont en correspondance bijective avec ceux de **N**, Cantor utilisait le symbole $\aleph_0$ ($\aleph$ ou « aleph », symbole qui appartient à l'alphabet hébreux ; le symbole $\aleph_0$ se lit « aleph zéro »). Et en langage mathématique, on peut donc écrire Card(**N**) = Card(**I**) = Card(**P**) = $\aleph_0$.

1655

On attribue à John Wallis la première utilisation du symbole du « nœud d'amour » noté ∞ pour désigner l'infini.

1874

Cantor applique un raisonnement rigoureux pour traiter le concept d'infini, et met en évidence différents types d'infini.

Dans les années 1960

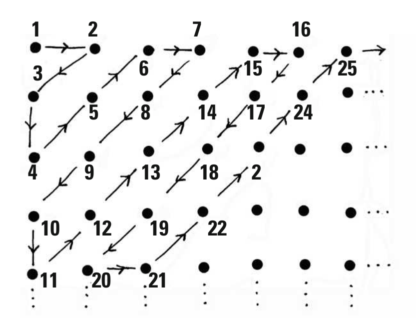
Abraham Robinson développe un modèle arithmétique non standard qui repose sur une théorie du calcul infinitésimal.

Tout ensemble qui peut être mis en bijection avec **N** s'appelle un ensemble « infini dénombrable». Dire qu'un ensemble est infini dénombrable signifie que l'on peut dresser la liste des éléments de l'ensemble. Par exemple, la liste des nombres impairs est simplement 1, 3, 5, 7, 9, … et nous savons quel élément est le premier, lequel est le deuxième, et ainsi de suite.

L'ensemble des fractions est-il infini dénombrable ? L'ensemble des fractions **Q** est un ensemble plus grand que **N** au sens où **N** peut être considéré comme un sous-ensemble de **Q**. Pouvons-nous établir la liste de tous les éléments de **Q** ? Pouvons-nous imaginer une liste où toutes les fractions (y compris les fractions négatives) figureraient quelque part ? L'idée qu'un ensemble si grand puisse être mis en bijection avec **N** semble impossible. On peut néanmoins y parvenir.

1	-1	2	-2	3	-3	4…
$\frac{1}{2}$	$\frac{-1}{2}$	$\frac{3}{2}$	$\frac{-3}{2}$	$\frac{5}{2}$	$\frac{-5}{2}$	$\frac{7}{2}$…
$\frac{1}{3}$	$\frac{-1}{3}$	$\frac{2}{3}$	$\frac{-2}{3}$	$\frac{4}{3}$	$\frac{-4}{3}$	$\frac{5}{3}$…
$\frac{1}{4}$	$\frac{-1}{4}$	$\frac{3}{4}$	$\frac{-3}{4}$	$\frac{5}{4}$	$\frac{-5}{4}$	$\frac{7}{4}$…
$\frac{1}{5}$	$\frac{-1}{5}$	$\frac{2}{5}$	$\frac{-2}{5}$	$\frac{3}{5}$	$\frac{-3}{5}$	$\frac{4}{5}$…
⋮	⋮	⋮	⋮	⋮	⋮	⋮

On commence avec une bijection. Au départ, on écrit sur une même ligne tous les nombres entiers, positifs et négatifs, en alternance. En dessous, on écrit toutes les fractions dont le dénominateur est égal à 2 mais on laisse de côté celles qui apparaissent déjà dans la rangée du dessus (comme 6/2 = 3). En dessous encore, on écrit les fractions dont le dénominateur est égal à 3, et on laisse encore une fois de côté toutes celles qui ont déjà été notées. On poursuit cette besogne sans fin, mais au moins, on sait où apparaît chaque fraction dans le diagramme. Par exemple, 209/67 est dans la 67e rangée, environ 200 places à la droite de 1/67.

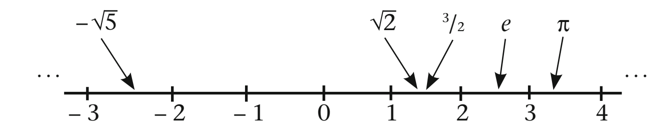


En disposant toutes les fractions de cette manière, potentiellement au moins, on peut construire une liste de dimension 1. Si on part de la rangée du haut et que l'on se déplace vers la droite, on ne peut jamais atteindre la deuxième rangée. Toutefois, on peut y parvenir en suivant un tracé en zigzag. On trouve la liste promise en suivant les flèches à partir de 1 :

1, –1, $^{1}/_{2}$, $^{1}/_{3}$,–$^{1}/_{2}$, 2, –2…

Chaque fraction, qu'elle soit positive ou négative, se trouve quelque part dans la liste et, réciproquement, sa position nous donne sa « partenaire » dans la liste de fractions. On peut donc conclure que l'ensemble de fractions **Q** est infini dénombrable et s'écrit Card(**Q**) = $\aleph_0$.

Dresser la liste des nombres réels Alors que l'ensemble des fractions totalise un grand nombre d'éléments qui viennent occuper la droite réelle, il existe aussi des nombres réels tels que $\sqrt{2}$, *e* et π qui ne sont pas des fractions. Ce sont les nombres irrationnels : ils « comblent les vides » pour nous donner la droite réelle **R**.



Une fois les vides comblés, on appelle l'ensemble **R** le « continuum ». Comment s'y prendre pour dresser une liste des nombres réels ? Dans un élan de pur génie, Cantor a montré que vouloir seulement énumérer les nombres réels compris entre 0 et 1 était une tentative vouée à l'échec. Cette nouvelle stupéfiante pour tous ceux que la constitution de listes passionne pourrait bien les amener à se demander pourquoi il est impossible de noter les uns après les autres les nombres réels d'un ensemble.

On suppose que vous ne croyez pas Cantor. Vous savez que chaque nombre entre 0 et 1 peut être exprimé sous la forme d'un développement décimal, comme par exemple

$$^1/_2 = 0{,}500\ 000\ 000\ 000\ 000\ 000\ldots \text{ et } ^1/_\pi = 0{,}318\ 309\ 886\ 183\ 790\ 671\ 53\ldots$$

Il vous faudrait donc dire à Cantor : « Voici ma liste de tous les nombres compris entre 0 et 1 », nombres que nous appellerons r_1, r_2, r_3, r_4, r_5, … Si vous n'êtes pas en mesure de produire une telle liste, alors vous donnerez raison à Cantor.

Imaginez que Cantor regarde votre liste et note en gras les nombres placés sur la diagonale :

$$r_1 : 0,\ a_1a_2a_3a_4a_5\ \ldots$$
$$r_2 : 0,\ b_1b_2b_3b_4b_5\ \ldots$$
$$r_3 : 0,\ c_1c_2c_3c_4c_5\ \ldots$$
$$r_4 : 0,\ d_1d_2d_3d_4d_5\ \ldots$$

Cantor dirait sûrement, « d'accord, mais où est le nombre $x = 0{,}x_1x_2x_3x_4x_5\ldots$ dont la première décimale x_1 est distincte de a_1, la seconde de b_2, la troisième de c_3 et ainsi de suite en suivant la diagonale ? ». Ce nombre x ainsi construit diffère de tous les nombres de votre liste au niveau d'une décimale, et c'est pourquoi il ne peut pas figurer dans votre liste. Cantor a raison.

En fait, une énumération de l'ensemble des nombres réels de **R** est impossible. L'ensemble **R** est donc pourvu d'un infini « plus grand » que celui de **Q**. Grand est simplement devenu plus grand.

l'idée clé
Une pluie d'infinités

08 Les nombres imaginaires

On peut sans problème imaginer des nombres. J'imagine parfois que je possède un million d'euros sur mon compte en banque et, une chose est sûre, c'est « un nombre imaginaire ». Cependant, l'utilisation mathématique de la notion d'imaginaire n'a rien à voir avec ces rêveries.

On pense que l'on doit l'appellation « imaginaire » au mathématicien et philosophe René Descartes qui l'a utilisée pour désigner les solutions curieuses de certaines équations, solutions qui n'étaient absolument pas des nombres ordinaires. Les nombres imaginaires existent-ils oui ou non ? C'est une question que les philosophes ont examinée sous toutes ses faces lorsqu'ils se sont penchés sur le mot « imaginaire ». Pour les mathématiciens, l'existence de nombres imaginaires n'est pas un problème. Ils font tout autant partie de notre vie quotidienne que le nombre 5 ou le nombre π. Les nombres imaginaires ne sont peut-être pas d'une grande utilité pour faire les soldes, mais allez demander à un concepteur d'avions ou à un ingénieur électricien, vous verrez que ces nombres sont d'une importance capitale. En ajoutant un nombre réel à un nombre imaginaire, on obtient ce que l'on appelle un « nombre complexe », ce qui semble tout de suite moins embarrassant d'un point de vue philosophique. La racine carrée de – 1 est le socle de la théorie des nombres complexes. Mais alors, quel est ce nombre qui, élevé au carré, donne – 1 ?

Si vous prenez un nombre non nul quelconque et le multipliez par lui-même (vous l'élevez au carré), vous obtenez toujours un nombre positif. Pas de problème si on élève des nombres positifs au carré mais qu'en est-il avec des nombres négatifs ? L'exemple $(-1) \times (-1)$ peut servir de test. Même si l'on a oublié cette règle des signes apprise à l'école qui nous dit que « moins par moins, ça fait plus », on peut quand même se souvenir que la réponse est soit – 1 soit + 1. Si, pour nous, $(-1) \times (-1)$ était égal à – 1, nous pourrions alors diviser chaque côté de l'équation par – 1 et en conclure que $-1 = 1$, ce qui est absurde. Nous devons donc en conclure que $(-1) \times (-1) = 1$, qui est positif. Le même raisonnement peut être tenu pour les nombres négatifs autres que – 1, et l'on en déduit que tout nombre réel élevé au carré ne peut jamais donner un résultat négatif.

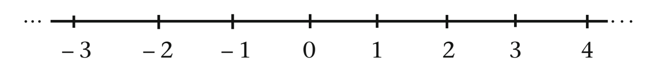
chronologie

1572
Rafael Bombelli utilise des nombres imaginaires dans ses calculs.

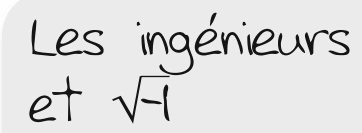
1777
Euler est le premier à utiliser le symbole *i* pour représenter la racine carrée de – 1.

Ce raisonnement fut à l'origine de tensions les premières années de l'apparition des nombres complexes au XVI[e] siècle. Ce problème surmonté, les mathématiques purent ainsi se soustraire aux contraintes qui pèsent sur les nombres ordinaires, et de vastes domaines d'investigation insoupçonnés jusque là s'ouvrirent alors. Le développement des nombres complexes a tout simplement permis de créer un système « complet » d'un niveau de perfection jamais atteint avec les nombres réels.

La racine carrée de – 1 Nous avons déjà vu que, si l'on s'en tient à la droite des nombres réels,



il n'existe pas de racine carrée de – 1 puisque le carré d'un nombre réel ne peut pas être négatif. Si l'on persiste à ne considérer que cette droite des réels, autant en rester là, continuer à les appeler des nombres imaginaires, aller prendre un café avec les philosophes, et ne plus nous en occuper. On pourrait aussi prendre la décision audacieuse d'accepter $\sqrt{-1}$ comme une nouvelle entité, que nous noterons i. Par cette unique opération de l'esprit, les nombres imaginaires peuvent prendre corps. Ce qu'ils sont est un mystère, mais nous croyons en leur existence. Nous savons au moins que $i^2 = -1$. Dans notre nouveau système de nombres, nous retrouvons donc tous ces bons vieux nombres réels tels que 1, 2, 3, 4, π, e, $\sqrt{2}$ et $\sqrt{3}$, auxquels viennent s'ajouter quelques petits nouveaux dans lesquels le nombre i apparaît, comme $1 + 2i$, $-3 + i$, $2 + 3i$, $1 + i\sqrt{2}$, $\sqrt{3} + 2i$, $e + i\pi$ et ainsi de suite.



Les ingénieurs, qui sont des gens pourtant très pragmatiques, ont trouvé une utilité aux nombres complexes. Lorsque Michael Faraday a découvert le courant alternatif dans les années 1830, les nombres imaginaires ont gagné une réalité physique. Dans ce domaine, on utilise la lettre j au lieu de i pour représenter $\sqrt{-1}$ parce que i représente le courant électrique.

Cette décision cruciale en mathématiques fut prise aux alentours du début du XIX[e] siècle, lorsque cette escapade à l'écart de la droite réelle, en dimension 1, nous a fait pénétrer dans ce nouveau plan étrange des nombres en dimension 2.

Additionner et multiplier Maintenant que nous avons à l'esprit les nombres complexes, à savoir des nombres de la forme $a + ib$, que pouvons-nous en faire ? Tout comme les nombres réels, on peut les additionner et les multiplier entre eux. L'addition se fait en additionnant leurs deux parties l'une après l'autre. Par conséquent, $2 + 3i$ ajouté à $8 + 4i$ donne $(2 + 8) + i(3 + 4)$, ce qui fait $10 + 7i$.

1806
Argand représente les nombres complexes dans un plan appelé « plan d'Argand-Cauchy ».

1811
Carl Friedrich Gauss travaille avec des fonctions de variables complexes.

1837
William R. Hamilton utilise les nombres complexes comme des couples ordonnés de nombres réels.

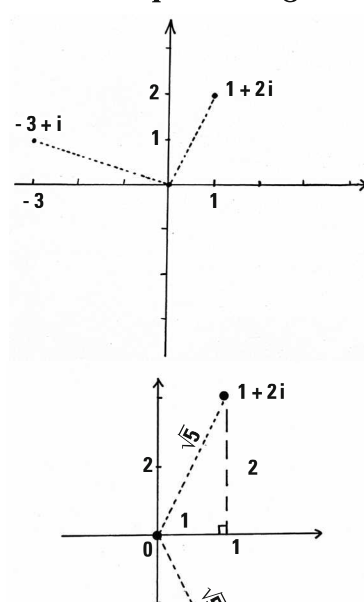
La multiplication est presque aussi simple. Pour multiplier $2 + 3i$ par $8 + 4i$, on multiplie d'abord chaque paire de symboles ensemble

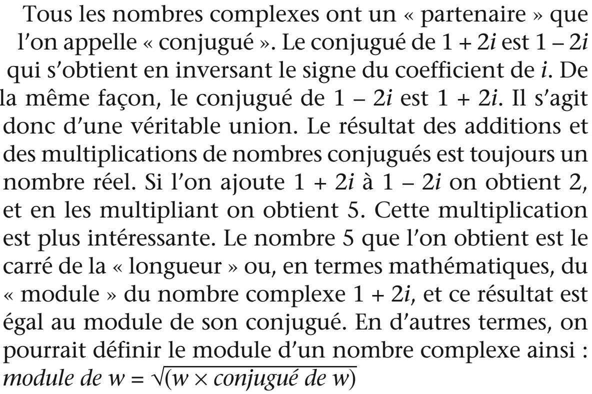
$$(2 + 3i) \times (8 + 4i) = (2 \times 8) + (2 \times 4i) + (3i \times 8) + (3i \times 4i)$$

et on additionne tous les termes obtenus, 16, $8i$, $24i$ et $12i^2$ (dans ce dernier terme on remplace i^2 par -1). Le résultat de la multiplication est donc $(16 - 12) + (8i + 24i)$, soit le nombre complexe $4 + 32i$.

Avec les nombres complexes, toutes les règles de l'arithmétique ordinaire sont respectées. La soustraction et la division sont toujours possibles (sauf avec le nombre complexe $0 + 0i$, mais elles n'étaient pas non plus autorisées pour le zéro avec les nombres réels). En fait, les nombres complexes bénéficient de toutes les propriétés des nombres réels sauf une. On ne peut pas séparer positifs et négatifs comme on le faisait avec les nombres réels.

Le plan d'Argand-Cauchy On voit clairement que les nombres complexes sont en dimension 2 si on les représente dans un plan muni d'un repère. Les nombres complexes $-3 + i$ et $1 + 2i$ peuvent être représentés dans ce que l'on appelle le plan d'Argand-Cauchy. Cette représentation des nombres complexes tient son nom de Jean-Robert Argand, mathématicien suisse et du français Augustin Cauchy, même si d'autres qu'eux travaillaient sur une idée similaire à peu près à la même époque.





Tous les nombres complexes ont un « partenaire » que l'on appelle « conjugué ». Le conjugué de $1 + 2i$ est $1 - 2i$ qui s'obtient en inversant le signe du coefficient de i. De la même façon, le conjugué de $1 - 2i$ est $1 + 2i$. Il s'agit donc d'une véritable union. Le résultat des additions et des multiplications de nombres conjugués est toujours un nombre réel. Si l'on ajoute $1 + 2i$ à $1 - 2i$ on obtient 2, et en les multipliant on obtient 5. Cette multiplication est plus intéressante. Le nombre 5 que l'on obtient est le carré de la « longueur » ou, en termes mathématiques, du « module » du nombre complexe $1 + 2i$, et ce résultat est égal au module de son conjugué. En d'autres termes, on pourrait définir le module d'un nombre complexe ainsi : *module de w* $= \sqrt{(w \times \textit{conjugué de } w)}$

Si on fait le calcul avec $-3 + i$ en guise de test, on trouve :

$$\textit{module de } (-3 + i) = \sqrt{(-3 + i) \times (-3 - i)} = \sqrt{(9 + 1)}$$

et donc le module de $-3 + i$ est égal à $\sqrt{10}$.

Si les nombres complexes ne sont plus considérés comme des nombres mystiques, on le doit surtout à Sir William Rowan Hamilton, le plus grand mathématicien irlandais

du XIXe siècle, le premier de son pays. Il reconnut que *i* n'était pas vraiment nécessaire pour la théorie. Pour lui, il servait seulement à occuper une place libre et l'on pouvait donc s'en débarrasser. Hamilton considérait les nombres complexes comme des « couples ordonnés » de nombres réels (a, b), faisant ainsi ressortir leur caractère bi-dimensionnel et ce, sans faire appel au mystique $\sqrt{-1}$.

Sans *i*, l'addition s'écrit $(2, 3) + (8, 4) = (10, 7)$

Et, de manière moins évidente, la multiplication s'écrit $(2, 3) \times (8, 4) = (4, 32)$

Le système de nombres complexes est un système très complet, caractéristique qui apparaît plus clairement lorsque l'on pense à ce que l'on appelle « les racines $n^{èmes}$ de l'unité » (pour les mathématiciens, « unité » signifie « 1 »). Ce sont les solutions de l'équation $z^n = 1$. À titre d'exemple, considérons l'équation $z^6 = 1$. Les deux racines $z = 1$ et $z = -1$ sont sur la droite des nombres réels (parce que $1^6 = 1$ et $(-1)^6 = 1$), mais où sont donc les quatre racines restantes, puisqu'il doit y en avoir six ? À l'image des deux racines réelles, les six racines complexes ont toutes un module égal à 1, et se trouvent donc toutes sur le cercle de rayon 1 et dont le centre est l'origine.

Il y a plus que cela. Si nous examinons $w = \frac{1}{2} + 3\,\frac{\sqrt{i}}{2}$, qui est la racine dans le premier quart de cercle, les racines successives (en allant dans le sens inverse des aiguilles d'une montre) sont $w^2, w^3, w^4, w^5, w^6 = 1$. Elles se trouvent toutes sur les sommets d'un hexagone régulier. De manière générale, les racines $n^{èmes}$ de l'unité sont toutes sur le cercle défini ci-dessus, et sur les « coins » ou « sommets » d'un polygone régulier à *n* côtés.

Extension des nombres complexes Une fois que les mathématiciens eurent à leur disposition les nombres complexes, ils cherchèrent instinctivement des généralisations. Les nombres complexes sont en dimension 2, mais qu'a-t-il de spécial, ce nombre 2 ? Pendant des années, Hamilton a cherché à construire des nombres en dimension 3 et à trouver une façon de les additionner et de les multiplier, mais en vain, et c'est seulement avec des nombres en dimension 4 qu'il y parvint. Peu après cette prouesse, on est passé des nombres en dimension 4 aux nombres en dimensions 8 (les nombres de Cayley, appelés aussi octaves ou octonions de Cayley). Beaucoup se sont interrogés sur les nombres en dimension 16 comme suite possible à toute cette histoire, mais 50 ans après l'exploit crucial de Hamilton, on prouva que c'était impossible.

l'idée clé
Nombres irréels aux réelles applications

09 Les nombres premiers

Les mathématiques sont une discipline puissante qui n'en finit pas de s'ingérer dans toutes les entreprises humaines, à tel point que l'on peut parfois avoir l'impression d'être dépassé. Il faut de temps en temps retourner aux bases. Cela signifie invariablement un retour aux nombres 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, … Peut-on faire encore plus simple ?

Eh bien, commençons avec $4 = 2 \times 2$. On peut donc fragmenter 4 en composants primaires. Peut-on décomposer ainsi tous les autres nombres quels qu'ils soient ? En voici quelques autres : $6 = 2 \times 3$, $8 = 2 \times 2 \times 2$, $9 = 3 \times 3$, $10 = 2 \times 5$, $12 = 2 \times 2 \times 3$. Ce sont des nombres composés car ils se construisent à partir des nombres de base 2, 3, 5, 7, … Les « nombres indécomposables » sont les nombres 2, 3, 5, 7, 11, 13, … On les appelle les nombres premiers. Un nombre premier est un nombre qui n'est divisible que par 1 et par lui-même. On peut alors se demander si 1 est un nombre premier. Selon cette définition, il devrait l'être, et il est vrai que par le passé, plusieurs grands mathématiciens ont traité 1 comme un nombre premier, mais aujourd'hui, les mathématiciens commencent leur liste de nombres premiers avec 2. Les théorèmes peuvent ainsi être formulés avec élégance. Pour nous aussi, le nombre 2 est le premier de la liste.

Prenons les premiers entiers naturels non nuls et soulignons les nombres premiers : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, … L'étude des nombres premiers nous ramène à ce qu'il y a de plus basique en mathématiques. Ils sont importants parce qu'ils en sont les « atomes ». De même que les éléments chimiques de base permettent de dériver tous les autres composés chimiques, les nombres premiers peuvent servir à la construction de composés mathématiques.

Le résultat mathématique autour duquel tout s'articule s'appelle pompeusement « le théorème de la décomposition en facteurs premiers des entiers ». Il dit que tout entier naturel supérieur ou égal à 2 s'écrit de manière unique en produit de nombres premiers. Nous avons vu que $12 = 2 \times 2 \times 3$ et qu'il n'existe aucune autre manière de le décomposer en produit de nombres premiers. Un tel résultat s'écrit souvent sous la forme condensée : $12 = 2^2 \times 3$. Autre exemple de ce type, 6 545 448 peut s'écrire $2^3 \times 3^5 \times 7 \times 13 \times 37$.

chronologie

300 av. J.-C.
Euclide, dans ses *Éléments*, donne la preuve de l'infinité des nombres premiers.

230 av. J.-C.
Ératosthène de Cyrène décrit une méthode pour cribler les nombres premiers et les séparer des autres entiers.

La chasse aux nombres premiers Il n'existe malheureusement pas de formule toute faite pour identifier les nombres premiers, dont l'apparence ne semble pas présenter de différence notable avec celle des autres entiers. L'une des premières méthodes pour y parvenir fut mise au point par un contemporain d'Archimède, plus jeune que lui cependant, qui passa la majeure partie de sa vie à Athènes : Ératosthène de Cyrène. Son calcul précis de la longueur de l'équateur suscita une grande admiration à l'époque. Il est aujourd'hui célèbre pour son « crible ». Ératosthène a imaginé que les nombres entiers s'étalaient devant lui. Il souligna 2 et raya tous les multiples de 2. Il passa ensuite à 3, le souligna et raya tous les multiples de 3. Avec ce procédé, il élimina tous les nombres composés. Les nombres soulignés non barrés qui restaient dans le crible étaient les nombres premiers.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

On peut donc trouver des nombres premiers, mais comment savoir si un nombre donné est un nombre premier ou non ? Qu'en est-il de 19 071 ou de 19 073 ? À l'exception des nombres premiers 2 et 5, un nombre premier doit se terminer par 1, 3, 7, ou 9, mais ce n'est pas une condition suffisante pour dire s'il s'agit d'un nombre premier. Il est difficile de savoir si un grand nombre qui se termine par 1, 3, 7 ou 9 est un nombre premier ou non sans essayer des facteurs possibles. Au fait, $19\,071 = 3^2 \times 13 \times 163$ et n'est donc pas un nombre premier, mais 19 073 en est un.

L'étude de la distribution des nombres premiers constitue un autre défi. Voyons combien il y a de nombres premiers entre 1 et 1 000, dans chaque segment de 100.

Intervalle	1–100	101–200	201–300	301–400	401–500	501–600	601–700	701–800	801–900	901–1000	1–1000
Nombre de nombres premiers	25	21	16	16	17	14	16	14	15	14	168

En 1792, Carl Friedrich Gauss, alors tout juste âgé de 15 ans, suggéra une formule notée $P(n)$ pour estimer le nombre de nombres premiers inférieurs ou égaux à un nombre donné n (ce théorème est aujourd'hui connu sous le nom de théorème des nombres premiers). Pour $n = 1\,000$, la formule donne une valeur approximative de 172. Il y en a en réalité 168, ce qui est inférieur à ce que donne l'estimation. On a toujours admis qu'il en allait ainsi pour toute valeur de n, mais les nombres premiers nous réservent souvent quelques surprises. On a ainsi montré que pour $n = 10^{371}$ (nombre gigantesque qui s'écrirait avec un 1 suivi de 371 zéros), le nombre de nombres premiers dépasse l'estimation. En fait, dans certaines régions, le nombre exact de nombres premiers peut être inférieur ou supérieur à l'estimation qui en est faite.

1742 ap. J.-C.
Goldbach conjecture que tout entier pair (supérieur ou égal à 4) est somme de deux nombres premiers.

1896
Le théorème des nombres premiers sur la distribution des nombres premiers est prouvé.

1966
Chen Jingrun n'est pas loin de confirmer la conjecture de Goldbach.

Combien ? Il y a une infinité de nombres premiers. Euclide nota dans ses *Éléments* (Livre 9, Proposition 20) que « les nombres premiers sont plus nombreux que toute multitude de nombres premiers proposée ». Voici la belle preuve qu'en donne Euclide :

Supposons que P est le plus grand nombre premier, et considérons le nombre

$$N = (2 \times 3 \times 5 \times \ldots \times P) + 1.$$

Ou bien N est un nombre premier ou bien il ne l'est pas. Si N est premier, c'est un nombre premier plus grand que P, ce qui est en contradiction avec notre supposition. Si N n'est pas premier, il doit être divisible par un nombre premier, par exemple p, qui figure dans la liste 2, 3, 5, …, P des nombres premiers. Cela signifie que p est diviseur de $N - (2 \times 3 \times 5 \times \ldots \times P)$. Mais ce nombre est égal à 1 et donc p est un diviseur de 1. C'est impossible puisque tous les nombres premiers sont supérieurs à 1. Ainsi, quelle que soit la nature de N, nous arrivons à une contradiction. Notre supposition de départ selon laquelle il y a un nombre premier supérieur à tous les autres est donc fausse. *Conclusion :* le nombre de nombres premiers est infini.

Les nombres premiers « s'étendent à l'infini », et pourtant cela n'a pas empêché certains de partir en quête du plus grand nombre premier connu. Le record était détenu il y a peu par ce gigantesque nombre premier de Mersenne qui s'écrit $2^{24\,036\,583} - 1$, et dont la valeur approximative est égale à $7{,}236 \times 10^{12}$ (ou environ 7 millions de millions).

L'inconnu De remarquables terres inconnues restent à découvrir dans le domaine des nombres premiers, tels que le « problème des nombres premiers jumeaux » ou la célèbre « conjecture de Goldbach ».

Les nombres premiers jumeaux sont des couples de nombres premiers consécutifs séparés par un seul nombre pair. Voici la liste des nombres premiers jumeaux compris entre 1 et 100 : (3, 5) ; (5, 7) ; (11, 13) ; (17, 19) ; (29, 31) ; (41, 43) ; (59, 61) ; (71, 73). Des calculs numériques ont permis de montrer qu'il y a 27 412 679 nombres premiers jumeaux inférieurs ou égaux à 10^{10}. Cela signifie que les nombres pairs qui séparent des nombres premiers jumeaux, comme 12 par exemple (qui a pour nombres jumeaux 11 et 13), ne constituent que 0,274% des nombres dans cet intervalle. Y-a-t-il une infinité de nombres premiers jumeaux ? Ce serait curieux si tel n'était pas le cas, mais personne n'a jusqu'à aujourd'hui réussi à en trouver une preuve.

Christian Goldbach a conjecturé que :

Tout nombre pair supérieur ou égal à 4 *est somme de deux nombres premiers.*

Le nombre 42 par exemple est un nombre pair qui peut s'écrire sous la forme 5 + 37. Peu importe qu'il soit aussi possible de l'écrire sous la forme 11 + 31, 13 + 29 ou 19 + 23. Une seule forme suffit. La conjecture est vraie pour une grande catégorie de nombres, mais la preuve n'a jamais pu être généralisée à l'ensemble des nombres entiers. Des progrès ont cependant été accomplis donnant ainsi l'impression qu'une preuve était à portée de main. Le mathématicien chinois Chen Jingrun permit une grande avancée. Son théorème dit que tout nombre pair suffisamment grand peut s'écrire comme somme d'un nombre premier et d'un nombre *presque* premier (nombre premier ou produit de deux nombres premiers).

Le nombre du numérologue

L'un des domaines les plus stimulants de la théorie des nombres concerne le « problème de Waring ». En 1770, Edward Waring, professeur à l'université de Cambridge, a formulé des problèmes qui portent sur la possibilité d'écrire les entiers comme sommes de puissances d'entiers. Dans ce cadre, arts magiques de la numérologie et science clinique des mathématiques se rencontrent là où se trouvent des nombres premiers, des sommes de carrés et des sommes de cubes. En numérologie, prenez ce nombre culte et sans égal, à savoir, le 666, le « nombre de la bête » dans l'Apocalypse. Il a quelques propriétés inattendues. C'est la somme des carrés des 7 premiers nombres premiers :

$$666 = 2^2 + 3^2 + 5^2 + 7^2 + 11^2 + 13^2 + 17^2$$

Les numérologues se plaisent toujours à faire remarquer que c'est la somme de cubes palindromiques, et, si cela ne suffit pas, que la clé de voûte 6^3 au centre est également la notation abrégée de $6 \times 6 \times 6$:

$$666 = 1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3 + 5^3 + 4^3 + 3^3 + 2^3 + 1^3$$

Le nombre 666 a tout pour plaire au numérologue.

Le grand théoricien des nombres Pierre de Fermat a prouvé que tout nombre premier de la forme $4k + 1$ peut s'écrire de manière unique comme somme de deux carrés (par exemple, $17 = 1^2 + 4^2$), alors que ceux de la forme $4k + 3$ (comme 19) ne le peuvent absolument pas. Joseph Lagrange a également prouvé un célèbre théorème mathématique sur les carrés : tout entier naturel positif est somme de quatre carrés. On a donc par exemple, $19 = 1^2 + 1^2 + 1^2 + 4^2$. On a exploré des puissances supérieures, rempli des livres de théorèmes, mais un grand nombre de problèmes restent ouverts.

Nous avons décrit les nombres premiers comme les « atomes des mathématiques ». Mais peut-être pensez-vous : « Les physiciens ont dépassé les atomes pour atteindre des unités plus fondamentales encore, comme les quarks. Et les mathématiques, se sont-elles arrêtées là ? » Si l'on s'en tient aux entiers naturels, 5 est un nombre premier et le restera, mais Gauss a fait une découverte de grande importance. Certains nombres premiers, 5 par exemple, peuvent se décomposer comme suit : $5 = (1 - 2i) \times (1 + 2i)$ où $i = \sqrt{-1}$ dans le système des nombres imaginaires. En tant que produits de deux entiers de Gauss, 5 et tous les nombres de ce type ne sont pas aussi indécomposables qu'on le pensait autrefois.

l'idée clé
Les atomes des mathématiques

10 Les nombres parfaits

En mathématiques, la quête de la perfection a conduit ceux qui s'y consacrent à explorer différents domaines. Il y a par exemple les carrés parfaits, dont la perfection n'a cependant rien à voir avec l'esthétique. L'adjectif « parfait » est ici employé pour signaler l'existence de carrés imparfaits. Autre exemple : certains nombres ont peu de diviseurs alors que d'autres en sont largement pourvus, mais, comme dans l'histoire de Boucle d'Or et des trois ours, certains nombres sont « juste comme il faut ». Lorsque la somme des diviseurs stricts d'un nombre est égal à ce nombre lui-même, ont dit alors qu'il est parfait.

Le philosophe grec Speusippe, qui reprit la direction de l'Académie après son oncle Platon, déclara que pour les Pythagoriciens, le nombre 10 avait tout pour prétendre à la perfection. Pourquoi ? Parce qu'entre 1 et 10, il y a autant de nombres premiers (à savoir 2, 3, 5, 7) que de nombres qui ne le sont pas (4, 6, 8, 9), et parce qu'il est le plus petit nombre à posséder cette propriété. Certains ont une idée bizarre de la perfection !

Les Pythagoriciens avaient semble-t-il une conception plus élaborée des nombres parfaits. Les propriétés mathématiques des nombres parfaits furent énoncées par Euclide dans ses *Éléments* et étudiées en profondeur par Nicomaque 400 ans plus tard. Une définition des nombres amiables et même de nombres sociables s'ensuivit. Cette définition reposait sur certains rapports qui existaient entre les nombres concernés et leurs diviseurs. Puis, ils formulèrent la théorie des nombres abondants et des nombres déficients, ce qui les amena à définir le concept de perfection.

Le caractère abondant d'un nombre est déterminé par ses diviseurs et fait jouer le lien entre multiplication et addition. Prenons le nombre 30 et considérons ses diviseurs stricts, c'est-à-dire tous les nombres qui le divisent exactement et qui sont strictement inférieurs à 30. Pour un nombre aussi petit que 30, on voit immédiatement que ses diviseurs stricts sont 1, 2, 3, 5, 6, 10 et 15. En faisant le total de ces diviseurs, on obtient 42. Le nombre 30 est abondant parce que la somme de ses diviseurs (42) est supérieure au nombre 30 lui-même.

chronologie

525 av. J.-C.
Les Pythagoriciens travaillent à la fois sur les nombres parfaits et les nombres abondants.

300 av. J.-C.
Le Livre 9 des *Éléments* d'Euclide traite des nombres parfaits.

100 ap. J.-C.
Nicomaque de Gérase donne une classification des nombres qui repose sur des nombres parfaits.

Rang	1	2	3	4	5	6	7
Nombre parfait	6	28	496	8 128	33 550 336	8 589 869 056	137 438 691 328

Les premiers nombres parfaits

Un nombre est déficient dans le cas inverse, c'est-à-dire si la somme de ses diviseurs stricts lui est inférieure. Ainsi, le nombre 26 est déficient parce que la somme de ses diviseurs stricts 1, 2, et 13 est égale à 16, résultat qui est strictement inférieur à 26. Les nombres premiers sont déficients parce que la somme de leurs diviseurs stricts est toujours égale à 1.

Un nombre qui n'est ni abondant ni déficient est parfait. La somme de ses diviseurs stricts est égale à lui-même. Le premier nombre parfait est 6. Ses diviseurs stricts sont 1, 2, 3 et si on les additionne, on obtient 6. Le nombre 6 et l'harmonie qui se dégage de la combinaison de ses différentes parties fut une telle source d'enchantement pour les Pythagoriciens qu'ils l'appelèrent « mariage, santé et beauté ». Il est une autre histoire sur le nombre 6 racontée par saint Augustin (354-430). Selon lui, la perfection du nombre 6 préexistait à la création du monde qui avait duré 6 jours, et ce justement parce que ce nombre était parfait.

Le nombre parfait suivant est 28. Ses diviseurs stricts sont 1, 2, 4, 7 et 14 et, en les additionnant, on obtient 28. Ces deux premiers nombres parfaits, 6 et 28, sont plutôt particuliers parce que l'on peut prouver que tous les nombres parfaits pairs se terminent par 6 ou 28. Après 28, il faut aller jusqu'à 496 pour trouver le nombre parfait suivant. Il est facile de vérifier qu'il est égal à la somme de ses diviseurs stricts : 496 = 1 + 2 +4 + 8 + 16 + 31 + 62 + 124 + 248. Pour trouver le nombre parfait suivant, il nous faut pénétrer dans la stratosphère numérique. Les cinq premiers nombres parfaits furent connus au XVIe siècle, mais on ignore toujours s'il en existe un qui serait plus grand que tous les autres, ou si leur nombre est illimité. L'opinion qui semble prédominer nous dit que la marche des nombres parfaits, comme celle des nombres premiers, se poursuit sans fin.

Les Pythagoriciens s'enthousiasmaient pour les liens géométriques. Si l'on dispose d'un nombre parfait de perles, on peut les arranger de manière à former un collier hexagonal. Avec 6 perles, on peut obtenir un hexagone simple en les plaçant à chaque coin, mais avec des nombres parfaits supérieurs, il faut insérer des colliers plus petits dans le grand collier.

1603

Pietro Cataldi trouve les 6e et 7e nombres parfaits, soient $2^{16} (2^{17} - 1) = 8\,589\,869\,056$ et $2^{18} (2^{19} - 1) = 137\,438\,691\,328$.

2006

Le grand projet de recherche de nombres premiers permet la découverte du 44e premier de Mersenne (qui contient presque 10 millions de chiffres) et pourtant il est encore possible de générer un nombre parfait plus grand encore.

Puissance	Résultat	Enlever 1 (nombre de Mersenne)	Nombre premier ?
2	4	3	premier
3	8	7	premier
4	16	15	non premier
5	32	31	premier
6	64	63	non premier
7	128	127	premier
8	256	255	non premier
9	512	511	non premier
10	1 024	1 023	non premier
11	2 048	2 047	non premier
12	4 096	4 095	non premier
13	8 192	8 191	premier
14	16 384	16 383	non premier
15	32 768	32 767	non premier

Les nombres de Mersenne Pour construire des nombres parfaits, on utilise une liste de nombres qui tiennent leur nom du Père Marin Mersenne, moine français qui étudia chez les Jésuites avec René Descartes. Les deux hommes s'intéressaient à la découverte de nombres parfaits. Les nombres de Mersenne, que l'on construit à partir de puissances de 2, sont des doubles tels que les nombres 2, 4, 8, 16, 32, 64, 128, 256… auxquels on soustrait une seule et unique unité. Les nombres de Mersenne sont de la forme $2^n - 1$. Toujours impairs, ils ne sont cependant pas toujours premiers. En revanche, on peut utiliser les nombres de Mersenne premiers pour construire des nombres parfaits.

Mersenne savait que si l'exposant de 2 n'était pas un nombre premier, alors le nombre de Mersenne ne pouvait pas être un nombre premier non plus, comme c'est le cas avec les puissances 4, 6, 8, 9, 10, 12, 14 et 15 dans notre tableau. Les nombres de Mersenne ne peuvent être premiers que si la puissance est elle-même un nombre premier, mais est-ce une condition suffisante ? Pour les quelques premiers cas, on obtient bien 3, 7, 31 et 127, qui sont tous premiers. Est-il donc vrai qu'un nombre de Mersenne formé avec un exposant premier est toujours premier lui aussi ?

De l'Antiquité jusqu'aux années 1500 environ, de nombreux mathématiciens pensaient qu'il en était ainsi. Mais les nombres premiers ne sont pas soumis à une telle simplicité. Par exemple, on a trouvé que pour la puissance 11 (qui est un nombre

De bons amis, tout simplement

Le mathématicien, qui a la tête sur les épaules, ne s'intéresse d'ordinaire pas à la mystique des nombres, mais la numérologie a encore de beaux jours devant elle. Les nombres amiables sont venus après les nombres parfaits même si l'on peut penser que les Pythagoriciens les connaissaient déjà. Plus tard, ils se sont avérés utiles pour établir des horoscopes où leurs propriétés mathématiques servaient à définir la nature de sentiments éthérés. Les deux nombres 220 et 284 sont des nombres amiables. Pourquoi ? Eh bien, les diviseurs de 220 sont 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, et 110 et si on les additionne, on obtient 284. Vous l'aviez deviné. Si vous calculez les diviseurs de 284 et les additionnez, vous obtenez 220. Ça, c'est de l'amitié.

premier), $2^{11} - 1 = 2\,047 = 23 \times 89$ et que, par conséquent, ce n'est pas un nombre premier. Il ne semble pas y avoir de règle. Les nombres de Mersenne $2^{17} - 1$ et $2^{19} - 1$ sont tous deux des nombres premiers, mais $2^{23} - 1$ n'est pas premier parce que

$2^{23} - 1 = 8\,388\,607 = 47 \times 178\,481$.

Travail de construction Une combinaison du travail d'Euclide et de celui d'Euler donne une formule qui permet même de produire des nombres parfaits pairs : n est un nombre parfait pair si et seulement si $n = 2^{p-1}(2^p - 1)$ où p est un nombre premier et $2^p - 1$ est un nombre de Mersenne premier.

Par exemple, $6 = 2^1\,(2^2 - 1)$, $28 = 2^2\,(2^3 - 1)$ et $496 = 2^4\,(2^5 - 1)$. Cette formule pour calculer les nombres parfaits pairs signifie que l'on peut les produire si l'on peut trouver des nombres premiers de Mersenne. Les nombres parfaits ont nargué et nargueront encore hommes et machines à un point que les premiers praticiens n'avaient pas imaginé. Au début du XIXe siècle, le collectionneur de nombres Peter Barlow écrivait que, selon lui, personne ne trouverait un nombre parfait d'Euler supérieur au nombre $2^{30}\,(2^{31} - 1) = 2\,305\,843\,008\,139\,952\,128$ parce que cela ne servirait pas à grand-chose. Il ne pouvait pas prévoir la puissance des ordinateurs modernes ni le besoin insatiable des mathématiciens de relever de nouveaux défis.

Nombres parfaits impairs On ignore si l'on trouvera un jour un nombre parfait impair. Descartes pensait que non, mais il arrive aux experts de se tromper. Le mathématicien anglais James Joseph Sylvester déclara que l'existence d'un nombre parfait impair « tiendrait presque du miracle » vu le grand nombre de conditions auxquelles il lui faudrait satisfaire. Il n'est pas très surprenant que Sylvester ait eu quelques doutes. C'est l'un des problèmes mathématiques les plus anciens, mais si un nombre parfait impair existe vraiment, on en sait déjà beaucoup à son sujet. Il lui faudrait au moins 8 diviseurs premiers, dont l'un serait supérieur à 1 million, et il devrait contenir au moins 300 chiffres.

Les premiers de Mersenne

Trouver les nombres premiers de Mersenne n'est pas chose facile. Pendant des siècles, de nombreux mathématiciens complétèrent cette liste dont l'histoire a connu des hauts et des bas, car erreurs et résultats corrects se mêlèrent et en constituent la base. Le grand Leonhard Euler a fourni en 1732 le 8e premier de Mersenne, à savoir $2^{31} - 1 = 2\,147\,483\,647$. La découverte du 23e premier de Mersenne, $2^{11\,213} - 1$, en 1963, fit la fierté du département de mathématiques de l'université de l'Illinois aux États-Unis qui l'annonça au monde en l'imprimant sur le timbre de l'université. Mais grâce à la puissance des ordinateurs, l'industrie des nombres premiers de Mersenne a pu accomplir de grands progrès. C'est ainsi qu'à la fin des années 1970, des lycéens, Laura Nickel et Landon Noll, ont découvert conjointement le 25e premier de Mersenne, et Noll le 26e. À ce jour, 49 nombres premiers de Mersenne nous sont connus.

l'idée clé
La mystique des nombres

11 Les nombres de Fibonacci

Dans le *Da Vinci Code*, le conservateur de musée Jacques Saunière, que l'auteur Dan Brown fait tuer, laisse derrière lui pour seul indice les huit premiers termes d'une suite de nombres. Il faut toute l'ingéniosité de la spécialiste en cryptologie Sophie Neveu pour réunir les nombres 13, 3, 2, 21, 1, 1, 8 et 5 et en comprendre la signification. Bienvenue dans la suite de nombres la plus célèbre de toutes les mathématiques.

La suite de nombres entiers de Fibonacci s'écrit ainsi :

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1 597, 2 584, …

Cette suite est bien connue pour ses nombreuses et curieuses propriétés. La plus fondamentale de ces propriétés, celle qui caractérise et définit ces nombres, dit que chaque terme est la somme des deux nombres qui le précèdent. Par exemple 8 = 5 + 3, 13 = 8 + 5, …, 2 584 = 1 587 + 987, et ainsi de suite. Il suffit de se souvenir qu'il faut commencer par les deux nombres 1 et 1, et à partir de là, on peut retrouver le reste de la suite. La suite de Fibonacci apparaît dans la Nature dans le nombre de spirales que forment les graines des fleurs de tournesol (on en compte par exemple 34 dans un sens, et 55 dans l'autre), et dans les proportions que donnent les architectes aux pièces et bâtiments qu'ils conçoivent. Des compositeurs de musique classique s'en sont inspirés, comme Bartók qui l'aurait utilisée pour composer sa *Suite de danses*. En musique contemporaine, Brian Transeau (plus connu sous son nom de scène BT) a intitulé « 1,618 » un morceau de son album *This Binary Universe* en référence à la divine proportion des nombres de Fibonacci, dont nous reparlerons un peu plus tard.

Origines La suite de Fibonacci est apparue dans le *Liber Abaci* publié par Léonard de Pise (Fibonacci) en 1202, mais ces nombres étaient probablement déjà connus en Inde avant cette date. Fibonacci a posé le problème de la reproduction des lapins :

Un couple de lapins adultes produit un couple de lapereaux chaque mois. Au début de l'année, il y a un couple de jeunes lapins. À la fin du premier mois, ils seront devenus

chronologie

1202
Léonard de Pise publie le *Liber Abaci* et les nombres de Fibonacci.

1724
Daniel Bernoulli exprime les nombres de la suite de Fibonacci en fonction du nombre d'or.

adultes, et à la fin du second mois le couple de lapins adultes est toujours vivant et aura produit un nouveau couple de jeunes lapins. Le processus de maturation et de reproduction se poursuit. Par miracle, aucun lapin ne meurt.

○ = couple de lapereaux
● = couple adulte

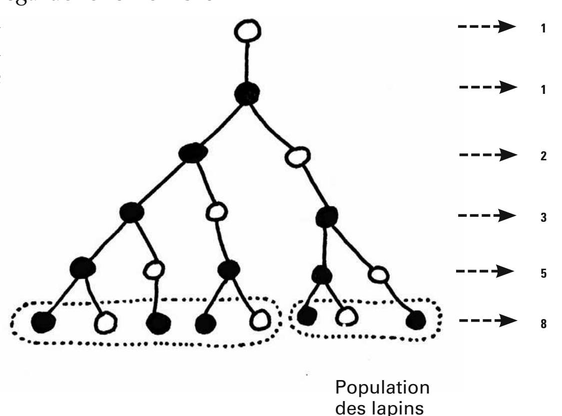
Fibonacci voulait savoir combien il y aurait de couples de lapins à la fin de l'année. Les différentes générations peuvent être représentées sur un « arbre généalogique ». Regardons le nombre de couples à la fin du mois de mai (le 5e mois). Nous voyons qu'il y en a 8. À ce niveau de l'arbre, le groupe de gauche

● ○ ● ● ○

est une réplique de la rangée supérieure, et le groupe de droite

● ○ ●

est une réplique de la rangée supérieure à celle-ci. On voit ainsi que la naissance de couples de lapins suit l'équation de base de Fibonacci :



Population des lapins

nombre après *n* mois = nombre après (*n* – 1) mois
+ nombre après (*n* – 2) mois.

Propriétés Voyons ce qui se passe si l'on additionne les termes de la suite :

1 + 1 = 2
1 + 1 + 2 = 4
1 + 1 + 2 + 3 = 7
1 + 1 + 2 + 3 + 5 = 12
1 + 1 + 2 + 3 + 5 + 8 = 20
1 + 1 + 2 + 3 + 5 + 8 + 13 = 33
…

Le résultat de chacune de ces sommes formera également une suite, que l'on peut placer sous la suite initiale, mais en la décalant :

Fibonacci	1	1	2	3	5	8	13	21	34	55	89…
Addition				2	4	7	12	20	33	54	88…

1923
Bartók compose sa *Suite de danses*, qui serait inspirée des nombres de Fibonacci.

1963
Le *Fibonacci Quarterly*, journal consacré à la théorie des nombres de Fibonacci, est fondé.

2007
Le sculpteur Peter Randall-Page crée la sculpture de 70 tonnes baptisée « Seed » en s'inspirant de la suite de Fibonacci pour le projet Eden en Cornouailles au Royaume-Uni.

L'addition de n termes de la suite de Fibonacci correspond au nombre de Fibonacci qui se trouve deux places plus loin et auquel on a retranché 1. Si vous voulez connaître le résultat de l'addition 1 + 1 + 2 + … + 987, il suffit d'ôter 1 de 2 584 : on obtient 2 583. Si l'on ajoute un nombre sur deux, par exemple 1 + 2 + 5 + 13+ 34, on obtient 55, qui est lui-même un nombre de Fibonacci. Si l'on choisit la solution alternative 1 + 3 + 8 + 21 + 55, on obtient 88 qui est un nombre de Fibonacci auquel on a retranché 1.

Les carrés de la suite de Fibonacci sont également intéressants. On obtient une nouvelle suite en multipliant chaque nombre de Fibonacci par lui-même et en additionnant les résultats obtenus.

Fibonacci	1	1	2	3	5	8	**13**	**21**	34	55	…
Carrés	1	1	4	9	25	64	169	441	1 156	3 025	…
Additions des carrés	1	2	6	15	40	104	**273**	714	1 870	4 895	…

Dans ce cas, additionner tous les carrés jusqu'au $n^{ème}$ nombre revient à multiplier le $n^{ème}$ nombre de la suite initiale de Fibonacci par le nombre qui le suit immédiatement. Par exemple,

$$1 + 1 + 4 + 9 + 25 + 64 + 169 = 273 = 13 \times 21$$

Les nombres de Fibonacci apparaissent aussi quand on ne s'y attend pas. Imaginons un porte-monnaie où sont mélangées des pièces de 1 et de 2 €. Que se passe-t-il si l'on veut compter le nombre de façons de sortir les pièces du porte-monnaie pour atteindre une somme particulière exprimée en euros ? Dans ce problème, l'ordre des actions est important. La somme 4 € peut être réalisée comme suit selon l'ordre de sortie des pièces : 1 + 1 + 1 + 1 ; 2 + 1 + 1 ; 1 + 2 + 1 ; 1 + 1 + 2 et 2 + 2. On peut procéder de 5 façons différentes en tout, ce qui correspond au 5e nombre de Fibonacci. Si vous prenez 20 €, il y a 6 765 façons de sortir des pièces de 1 et de 2 €, ce qui correspond au 21e nombre de Fibonacci ! On voit ici toute la puissance d'idées mathématiques simples.

Le nombre d'or Si l'on regarde le rapport des termes formé par la suite de Fibonacci en divisant un terme par celui qui le précède, on trouve une autre propriété remarquable des nombres de Fibonacci. Faisons l'expérience avec les quelques termes 1, 1, 2, 3, 5, 8, 13, 21, 34, 55.

1/1	2/1	3/2	5/3	8/5	13/8	21/13	34/21	55/34
1,000	2,000	1,500	1,333	1,600	1,625	1,615	1,619	1,617

Très rapidement, les rapports obtenus se rapprochent d'une valeur connue sous le nom de nombre d'or, nombre célèbre en mathématiques, désigné par la lettre grecque Φ. Il a sa place parmi les meilleures constantes mathématiques telles que π et e, et a pour valeur exacte

$$\Phi = \frac{1+\sqrt{5}}{2}$$

ce qui est à peu près égal à 1,618 033 988… Avec un peu plus de travail, on peut montrer que tout nombre de Fibonacci peut s'écrire en fonction de Φ.

Les connaissances sur la suite de Fibonacci sont vastes, mais pourtant un grand nombre de questions restent sans réponse. Les premiers nombres premiers de la suite de Fibonacci sont 2, 3, 5, 13, 89, 233, 1 597, mais on ignore si la suite en contient une infinité.

Ressemblances familiales La suite de Fibonacci occupe la place d'honneur au sein d'une vaste famille de suites similaires. Parmi elles, celle que l'on peut associer à un problème de population bovine est spectaculaire. Contrairement aux couples de jeunes lapins de Fibonacci qui deviennent en un mois des lapins capables de se reproduire, les jeunes bovins passent par une étape intermédiaire avant de devenir adultes. Seuls les couples adultes peuvent se reproduire. La suite pour les couples de bovins est la suivante :

1, 1, 1, 2, 3, 4, 6, 9, 13, 19, 28, 41, 60, 88, 129, 189, 277, 406, 595, …

Les générations sautent ainsi une valeur. Par exemple, on a 41 = 28 + 13 et 60 = 41 + 19. Cette suite de bovins, appelée suite de Lamé, a des propriétés similaires à celle de Fibonacci. Les rapports obtenus en divisant un terme par le terme précédent tendent vers une limite que l'on note avec la lettre grecque psi, et que l'on écrit Ψ, où

$$\Psi = 1{,}465\ 571\ 231\ 876\ 768\ 026\ 65\ldots$$

C'est ce que l'on appelle le « super nombre d'or ».

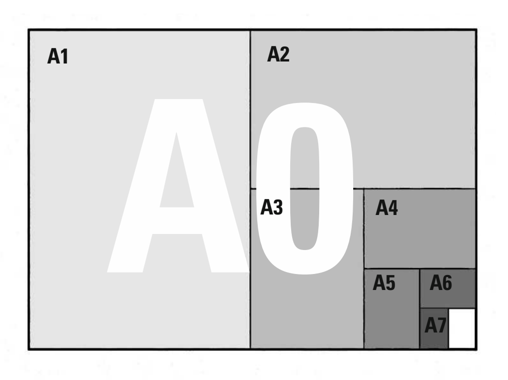
Cheptel

l'idée clé
Décryptage du Da Vinci Code

12 Les rectangles d'or

Nous sommes entourés de rectangles : les immeubles, les photos, les fenêtres, les portes, et jusqu'à ce livre sont des rectangles. Les artistes en font aussi usage. Piet Mondrian, Ben Nicholson et bien d'autres encore, qui ont évolué vers l'art abstrait, en ont tous utilisés d'un genre ou d'un autre dans leurs tableaux. Quel est donc le plus beau rectangle de tous ? Est-ce celui de Giacometti, long et étroit, ou est-ce l'un de ces rectangles presque carrés ? Ou est-ce encore un rectangle intermédiaire entres ces deux extrêmes ?

Mais la question a-t-elle vraiment un sens ? Oui, pensent ceux qui ont la conviction que certains rectangles sont plus « parfaits » que d'autres. De tous, le rectangle d'or est peut-être celui qui remporte l'adhésion du plus grand nombre. Parmi tous les rectangles que l'on pourrait choisir en raison de leurs proportions, parce qu'il ne s'agit pas d'autre chose, le rectangle d'or est une figure très particulière qui a inspiré des artistes, des architectes, et des mathématiciens. Examinons d'autres types de rectangles pour commencer.



Papier mathématique Si l'on prend une feuille de format A4, dont les dimensions sont de 210 mm sur 297 mm, le rapport entre la longueur et la largeur est de 297/210, ce qui vaut approximativement 1,4142. Pour tout format international de la série A, la longueur sera toujours égale à $1{,}4142 \times b$, b désignant la largeur de la feuille. Donc, pour un format A4, $b = 210$ mm, alors que pour le format A5, $b = 148$ mm. Le système de classification utilisé pour désigner le format des feuilles présente une propriété extrêmement intéressante qui n'apparaît pas si l'on prend des dimensions quelconques de feuille de papier. Si l'on plie en deux une feuille A4, les

chronologie

Vers 300 av. J.-C.
Le rapport extrême et intermédiaire est publié dans les *Éléments* d'Euclide.

1202 ap. J.-C.
Léonard de Pise publie le *Liber Abaci*.

deux petits rectangles ainsi formés sont proportionnellement identiques au rectangle initial. Ce sont les modèles réduits de ce même rectangle.

Ainsi, une feuille A4 pliée en deux donne deux feuilles de format A5. De la même façon, un format A5 donne deux formats A6. À l'inverse, une feuille A3 est faite de 2 feuilles A4. Plus le nombre est petit, plus la feuille est grande. Comment avons-nous su que le nombre particulier 1,4142 conviendrait ? Plions un rectangle dont la longueur nous est cette fois inconnue. Si l'on considère que la largeur d'un rectangle vaut 1, et si l'on désigne par x la mesure de la longueur, alors le rapport de la longueur à la largeur est de $x/1$. Si l'on plie maintenant le rectangle, le rapport de la longueur à la largeur du rectangle plus petit est égal à $1/(x/2)$, soit $2/x$. Avec les formats A, nos deux rapports doivent représenter la même proportion, de sorte que l'on obtient une équation du type $x/1 = 2/x$ ou $x^2 = 2$. La vraie valeur de x est donc $\sqrt{2}$, soit 1,4142 en valeur approchée.

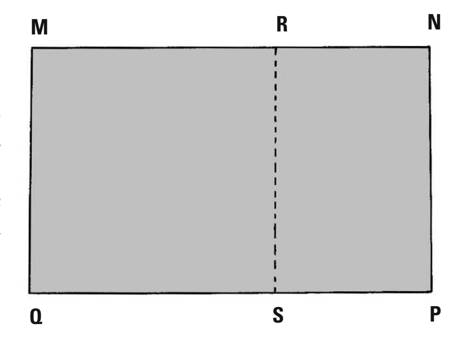
Or mathématique Le rectangle d'or est différent du format A, mais il ne l'est pas tant que cela. Cette fois, le rectangle est plié le long de la droite (RS) sur le diagramme de sorte que les points MRSQ forment les quatre sommets d'un carré.

La propriété essentielle du rectangle d'or est que le rectangle *RNPS* restant est proportionnel au grand rectangle, de sorte qu'il devrait être une réplique miniature du grand rectangle.

Comme ci-dessus, on dira que la largeur MQ = MR du grand rectangle est de longueur 1 unité et l'on notera x la longueur du grand côté [MN]. Le rapport longueur sur largeur est encore de $x/1$. Cette fois, la largeur du petit rectangle RNPS est égale à MN – MR, soit $x - 1$ et donc le rapport longueur sur largeur de ce rectangle est égal à $1/(x - 1)$.

La mise en équation donne $\frac{x}{1} = \frac{1}{x-1}$ que l'on peut écrire $x^2 = x + 1$. Une valeur approchée de la solution positive est 1,618. Il est facile de le vérifier. Si l'on tape 1,618, et si l'on multiplie ce nombre par lui-même, la calculatrice donne 2,618, ce qui est égal à $x + 1 = 2,618$. C'est le célèbre nombre d'or que l'on désigne par la lettre grecque phi, notée Φ. Sa définition et sa valeur approchée est donnée par

$$\Phi = \frac{1+\sqrt{5}}{2} = 1{,}618\ 033\ 988\ 749\ 894\ 848\ 20\ldots$$



et ce nombre est lié à la suite de Fibonacci et au problème des lapins (voir page 45).

1509
Pacioli publie *La Divine Proportion*.

1876
Fechner travaille sur des expériences psychologiques pour déterminer les proportions du rectangle le plus « esthétique ».

1975
Le comité technique ISO (Organisation Internationale de Normalisation) définit le format de la série A des feuilles de papier.

Le choix de l'or Voyons maintenant si l'on peut construire un rectangle d'or. Nous commencerons avec notre carré MQSR de côté unité et nous noterons O le milieu de [QS]. La longueur OS = 1/2, et donc, selon le théorème de Pythagore (voir page 84) dans le triangle ORS, on a

$$OR = \sqrt{\left(\frac{1}{2}\right)^2 + 1^2} = \frac{\sqrt{5}}{2}$$

En utilisant un compas centré en O, on peut tracer l'arc *RP* et l'on trouve que $OP = OR = \frac{\sqrt{5}}{2}$. On termine donc avec $QP = \frac{1}{2} + \frac{\sqrt{5}}{2} = \Phi$, ce qui est le résultat souhaité : la « section d'or » ou le côté du rectangle d'or.

Histoire On entend toutes sortes de choses sur le nombre d'or. Lorsque l'on se rend compte de ses propriétés mathématiques et de l'intérêt qu'elles représentent, on le voit dans des endroits inattendus, et même là où il n'est pas. Pire, on peut aller jusqu'à affirmer que le nombre d'or préexistait à l'objet, que les musiciens, les architectes et les artistes l'avaient à l'esprit au moment de la création. C'est ce que l'on pourrait appeler « le nombre d'orisme ». Passer des nombres à des affirmations générales sans apporter de preuve est dangereux.

Prenez le Parthénon à Athènes. À l'époque de sa construction, le nombre d'or était certainement connu, mais cela ne signifie pas qu'il a servi de base à sa conception. Effectivement, sur la façade du Parthénon, le rapport de la largeur à la hauteur (fronton triangulaire inclus) est égal à 1,74 ce qui n'est pas très loin de 1,618, mais est-ce suffisamment proche pour prétendre que la présence du nombre d'or est délibérée ? Certains soutiennent que le fronton ne doit pas être pris dans les calculs, et ainsi, le rapport de la largeur à la hauteur est égal au nombre entier 3.

Dans son ouvrage *De divina proportione* publié en 1509, Luca Pacioli a « découvert » des liens entre les caractéristiques divines et les propriétés de la proportion telle qu'elle est définie par Φ. Il la nomma « proportion divine ». Pacioli était un moine franciscain auteur d'ouvrages mathématiques qui ont fait autorité. Il est parfois considéré comme le « père de la comptabilité » parce qu'il a popularisé la méthode en partie double utilisée par les marchands vénitiens. Il est également connu pour avoir enseigné les mathématiques à Léonard de Vinci. À l'époque de la Renaissance, le domaine du nombre d'or acquit un statut presque mystique – l'astronome Johannes Kepler voyait en lui un « joyau » mathématique. Plus tard, un grand psychologue allemand du nom de Gustav Fechner mesura des milliers de formes rectangulaires (cartes à jouer, livres, fenêtres) pour arriver à la conclusion que le rapport le plus utilisé était proche de Φ.

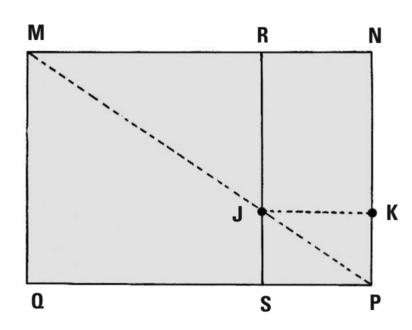
Le Corbusier était fasciné par le rectangle, élément central dans ses conceptions architecturales, et par le rectangle d'or en particulier. Il attachait beaucoup d'importance à l'harmonie et à l'ordre, qu'il trouvait dans les mathématiques. Il regardait l'architecture avec des yeux de mathématicien. Il est l'auteur du « modulor », système de mesure basé sur une théorie des proportions. Cet outil servait en fait à la production en série de rectangles d'or, forme qu'il utilisait pour concevoir ses plans. Le Corbusier s'est inspiré de Léonard de Vinci, qui avait lui-même étudié les réalisations de l'architecte romain Vitruve, pour lequel les proportions présentes dans le corps humain étaient d'une grande importance.v

Autres formes Il existe aussi un « super rectangle d'or » dont la construction est proche de celle du rectangle d'or.

Voici comment on construit le super rectangle d'or MQPN. Comme précédemment, MQSR est un carré de côté 1. Tracez la diagonale [MP] et notez J son intersection avec (RS). Puis, tracez une droite passant par J, parallèle à (RN), et qui coupe (NP) en K. On appellera y la longueur RJ et x la longueur MN. On a RJ/MR = NP/MN (car les triangles MRJ et MNP sont semblables), ce qui s'écrit

$$\frac{y}{1} = \frac{1}{x}$$

et donc $xy = 1$. On dit alors que x et y sont « inverses ». On obtient le super rectangle d'or en construisant le rectangle RJKN dont les côtés sont proportionnels à ceux du rectangle d'origine MQPN, c'est-à-dire



$$\frac{y}{x-1} = \frac{x}{1}.$$

En utilisant le fait que $xy = 1$, on peut conclure que la longueur du super rectangle d'or x est solution de l'équation « cubique » $x^3 = x^2 + 1$, qui ressemble à l'équation $x^2 = x + 1$ (équation qui définit le rectangle d'or). L'équation cubique a une solution réelle positive Ψ (en remplaçant x par le symbole plus courant Ψ) dont la valeur est

$$\Psi = 1{,}465\ 571\ 231\ 876\ 768\ 026\ 65\ldots$$

nombre associé à la suite de Lamé (voir page 47). Le rectangle d'or est constructible à la règle et au compas, contrairement au super rectangle d'or.

l'idée clé
Proportions divines

13 Le triangle de Pascal

Le nombre 1 est important mais qu'en est-il de 11 ? Il l'est aussi, et il en va de même pour 11 × 11 = 121, 11 × 11 × 11 = 1 331 et pour toutes les puissances supérieures de 11. On peut les présenter ainsi :

11
121
1 331
14 641

On obtient alors les premières lignes du triangle de Pascal. Mais où le trouver ?

On pose maintenant $11^0 = 1$ pour se faire plaisir, et on espace tous les chiffres. Ainsi, 14 461 s'écrit

1 4 6 4 1.

Le triangle de Pascal tient sa renommée en mathématiques de ses qualités de symétrie et des nombreuses relations cachées qu'il entretient avec d'autres domaines mathématiques. Ainsi pensait Pascal en 1653 qui observait alors qu'il ne pourrait toutes les traiter dans un article unique. Les nombreux liens qui existent entre le triangle de Pascal et les autres branches mathématiques en ont fait un objet digne de vénération dont les origines remontent cependant à une période bien antérieure. En réalité, Pascal n'est pas l'inventeur du triangle qui porte son nom puisqu'il était connu de savants chinois au XIIIe siècle de notre ère.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 0 0 5 1

Le triangle de Pascal

Le triangle de Pascal se construit en démarrant par le haut. Commencez avec le chiffre 1 et placez deux autres 1 de chaque côté du premier mais sur la ligne du dessous. Pour poursuivre la construction, on place le chiffre 1 à chaque extrémité des lignes alors que les nombres à l'intérieur du triangle s'obtiennent en faisant la somme des

chronologie

Vers 500 av. J.-C.
Des preuves fragmentaires en sanscrit attestent de l'existence du triangle de Pascal.

Vers 1070 ap. J.-C.
Omar Khayyam découvre le triangle qui, dans certains pays, porte son nom.

deux nombres placés juste au-dessus. Pour obtenir 6 dans la cinquième ligne par exemple, on additionne les deux 3 de la ligne supérieure. Le mathématicien G. H. Hardy déclara que « le mathématicien, à l'instar du peintre ou du poète, crée des formes ». Le triangle de Pascal en est un bon exemple.

Liens avec l'algèbre Le triangle de Pascal repose sur de vraies mathématiques. Par exemple, si l'on développe $(1 + x) \times (1 + x) \times (1 + x) = (1 + x)^3$, on obtient $1 + 3x + 3x^2 + x^3$. Regardez bien et vous verrez que, dans cette expression, les nombres en facteur de x sont identiques à ceux qui apparaissent dans les lignes correspondantes du triangle de Pascal. Le schéma est le suivant :

$(1 + x)^0$						1					
$(1 + x)^1$					1		1				
$(1 + x)^2$				1		2		1			
$(1 + x)^3$			1		3		3		1		
$(1 + x)^4$		1		4		6		4		1	
$(1 + x)^5$	1		5		10		10		5		1

Si l'on additionne les nombres d'une ligne quelconque du triangle de Pascal, on obtient toujours une puissance de 2. Par exemple, dans la cinquième ligne en partant du haut, $1 + 4 + 6 + 4 + 1 = 16 = 2^4$. De même pour la colonne de gauche ci-dessus si l'on prend $x = 1$.

Propriétés La première propriété évidente du triangle de Pascal est sa symétrie. Si l'on trace une droite verticale qui le traverse en son milieu, le triangle possède une « symétrie inversée » – la partie gauche est identique à celle de droite. On peut ainsi parler de « diagonales » simples, parce qu'une diagonale de direction nord-est sera identique à une diagonale de direction nord-ouest. Sous la diagonale constituée des différents 1, se trouve la diagonale constituée des nombres 1, 2, 3, 4, 5, 6… En dessous de celle-ci, se trouvent les nombres triangulaires 1, 3, 6, 10, 15, 21… (les nombres que l'on obtient en faisant le total des points disposés en triangles). Dans la diagonale en dessous, on a les nombres tétraédriques 1, 4, 10, 20, 35, 56… Ces nombres correspondent aux tétraèdres (« triangles en dimension 3 », ou, si vous préférez, au nombre de boulets de canon que l'on peut placer sur des bases triangulaires de plus en plus grandes). Et qu'en est-il des « quasi diagonales » ?

Si l'on ajoute les nombres qui se trouvent sur les droites qui traversent le triangle (droites qui ne sont ni des lignes ni de vraies diagonales), on obtient la suite 1, 2, 5, 13, 34…

Les quasi diagonales du triangle de Pascal

1303
Zhu Shijie définit le triangle de Pascal et montre comment obtenir certaines suites.

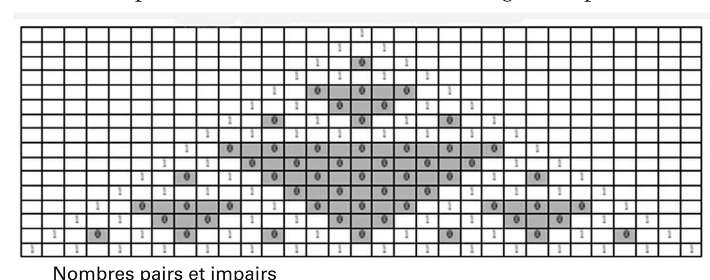
1664
L'article de Pascal sur les propriétés du triangle est publié à titre posthume.

1714
Leibniz examine le triangle harmonique.

Chacun de ces nombres est égal à trois fois le nombre précédent moins le nombre qui précède ce dernier. Par exemple, 34 = 3 × 13 – 5. En suivant cette méthode, le nombre suivant sera 3 × 34 – 13 = 89. On a écarté une « quasi diagonale » sur deux, à savoir celles qui commencent par 1, 1 + 2 = 3, mais ces dernières nous donneront la suite **1**, **3**, **8**, **21**, **25**, **55**…, nombres générés par cette même règle du « trois fois moins 1 ». Nous pouvons donc produire le nombre suivant de la suite, à savoir 3 × 55 – 21 = **144**. Mais il y a mieux. Si l'on intercale ces deux suites données par ces « quasi diagonales », on obtient les nombres de Fibonacci :

1, **1**, 2, **3**, 5, **8**, 13, **21**, 34, **55**, 89, **144**, …

Combinaisons de Pascal Les nombres de Pascal sont solutions de quelques problèmes de dénombrement. Imaginez 7 personnes dans une pièce. Appelons-les **A**lice, **C**atherine, **E**mma, **G**aspard, **J**érôme, **M**athieu, et **T**homas. Combien existe-t-il de façons différentes de les placer par groupes de trois ? On pourrait regrouper **A**, **C**, **E**, ou encore **A**, **C**, **T**. Les mathématiciens notent par commodité C_n^r le nombre de la n^e rangée à la r^e position (en commençant à $r = 0$) du triangle de Pascal. La réponse à notre question est C_7^3. Le 3e nombre de la 7e rangée du triangle est 35. Si l'on choisit un groupe de 3, on sélectionne du même coup un groupe de 4 personnes « non choisies ». Cela explique que $C_7^4 = 35$ également. En général, $C_n^r = C_n^{n-r}$, ce qui découle de la symétrie du triangle de Pascal.



Nombres pairs et impairs dans le triangle de Pascal

Le triangle de Sierpińskі

Les 0 et les 1 Dans le triangle de Pascal, on voit que les nombres placés à l'intérieur forment un dessin qui varie selon que les nombres sont pairs ou impairs. Si l'on substitue 1 à chaque nombre impair et 0 à chaque nombre pair, on obtient une représentation similaire au remarquable ensemble fractal connu sous le nom de triangle de Serpin'ski (voir page 102).

Ajout de signes On peut représenter le triangle de Pascal qui correspond aux puissances de $(-1 + x)$ c'est-à-dire $(-1 + x)^n$. Dans ce cas, le triangle n'est pas complètement symétrique par rapport à la droite verticale, et au lieu de donner des puissances de 2, la somme des nombres de chaque ligne donne 0. Cependant, ce sont les diagonales qui sont intéressantes ici. La diagonale de direction sud-ouest qui s'écrit 1, – 1, 1, – 1, 1, – 1, 1, – 1, … est constituée des coefficients du développement

$$(1 + x)^{-1} = 1 - x + x^2 - x^3 + x^4 - x^5 + x^6 - x^7 + \ldots$$

Ajout de signes

alors que les termes de la diagonale suivante sont les coefficients du développement

$$(1 + x)^{-2} = 1 - 2x + 3x^2 - 4x^3 + 5x^4 - 6x^5 + 7x^6 - 8x^7 + \dots$$

Le triangle harmonique de Leibniz L'Allemand Gottfried Leibniz, mathématicien à l'esprit universel, déco uvrit un ensemble étonnant de nombres arrangés en forme de triangle. Les nombres de Leibniz sont disposés symétriquement le long de la médiane. Mais, contrairement au triangle de Pascal, le nombre d'une ligne s'obtient par addition des deux nombres placés en dessous de lui. Par exemple, 1/30 + 1/20 = 1/12. Pour construire ce triangle, on peut démarrer d'en haut et progresser de la gauche vers la droite en faisant une soustraction : on connaît 1/12 et 1/30 et donc 1/12 – 1/30 = 1/20, nombre placé à la droite de 1/30. Vous avez peut-être observé que la diagonale extérieure est la célèbre série harmonique

Le triangle harmonique de Leibniz

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \cdots$$

mais la seconde diagonale est ce que l'on appelle la série Leibnizienne

$$\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \cdots + \frac{1}{n \times (n+1)}$$

qui, après quelque manipulation astucieuse, s'avère être égale à n/(n +1). De la même manière que précédemment, on peut écrire ces nombres de Leibniz sous la forme B_n^r

pour représenter le n^e nombre dans le r^e rang. Ils ont un lien avec les nombres ordinaires de Pascal C_n^r via la formule :

$$B_n^r \times C_n^r = \frac{1}{n+1}$$

Le triangle de Pascal est étroitement lié à de nombreux domaines mathématiques – géométrie moderne, analyse combinatoire, et algèbre pour n'en citer que trois. Plus que cela, c'est un exemple typique de ce en quoi consistent les mathématiques, à savoir une recherche constante de régularité et d'harmonie, recherche qui renforce notre compréhension de la discipline même.

l'idée clé
La fontaine des nombres

14 L'algèbre

L'algèbre met à notre disposition une méthode particulière de résolution de problèmes, une méthode par déduction tout à fait astucieuse. Il s'agit d'opérer un raisonnement déductif « à rebours ». Prenons un cas simple : au nombre 25, ajoutons 17. On obtient 42. C'est un exemple de déduction directe. On nous donne les nombres et il nous suffit de les additionner. Mais supposons maintenant une réponse donnée, à savoir 42, et une question différente. Nous voulons maintenant connaître le nombre qui ajouté à 25 donne 42. C'est là qu'intervient le raisonnement à rebours. On veut trouver cette valeur de x qui résout l'équation $25 + x = 42$. On soustrait alors 25 de 42 pour trouver cette valeur.

Depuis des siècles, les maîtres d'école posent ce genre de problèmes que la méthode algébrique permet de résoudre :

Ma nièce Mélissa est âgée de 6 ans et moi de 40 ans.
Quand aurai-je trois fois son âge ?

La solution pourrait s'obtenir par tâtonnement mais l'algèbre est une méthode plus économique. Dans x années, Mélissa sera âgée de $6 + x$ années et moi de $40 + x$ années. J'aurai trois fois son âge lorsque $3 \times (6 + x) = 40 + x$.

On développe le membre de gauche de l'équation et l'on obtient $18 + 3x = 40 + x$, puis on fait passer tous les x d'un côté et tous les nombres de l'autre. On trouve alors $2x = 22$, ce qui signifie que $x = 11$. Quand j'aurai 51 ans, Mélissa aura 17 ans. Magique !

Et s'il s'agissait de savoir à quel moment je serai deux fois plus âgé qu'elle ? On peut utiliser la même approche, en résolvant cette fois l'équation

$$2 \times (6 + x) = 40 + x.$$

On obtient alors $x = 28$. Elle aura 34 ans lorsque j'en aurai 68. Toutes les équations ci-dessus appartiennent au type le plus simple : on les appelle les équations « du premier degré ». Elles ne comportent aucun terme tel que x^2 ou x^3, et sont donc faciles à résoudre. Les équations qui contiennent des termes tels que x^2 sont des équations « du second degré » ou équations « quadratiques », tandis que celles qui contiennent

chronologie

1950 av. J.C
Les Babyloniens travaillent avec des équations du second degré.

250 ap. J.-C.
Diophante d'Alexandrie publie *Arithmetica*.

825
Al-Khwarizmi donne le nom « algèbre », qui est dérivé de « *al-jabr* », aux mathématiques.

des termes du type x^3 sont dites « de degré trois ». Dans le passé, on représentait x^2 sous la forme d'un carré et, un carré étant doté de quatre côtés, on utilisait alors l'adjectif « quadratique » ; quant à x^3, on le représentait sous la forme d'un cube.

Les mathématiques se sont profondément transformées lorsque, de science de l'arithmétique, elles sont devenues science des symboles avec l'algèbre. Passer des nombres aux lettres représente un effort intellectuel considérable qui en vaut cependant la peine.

Les origines L'algèbre occupait une place importante dans le travail des érudits islamiques du IXe siècle. Al-Khwarizmi écrivit un traité de mathématiques qui contenait le mot arabe *al-jabr*. Traitant de problèmes concrets en termes d'équations du premier et du second degré, la « science des équations » d'Al-Khwarizmi nous a donné le mot « algèbre ». Bien plus tard encore, Omar Khayyam est célèbre pour avoir écrit le *Rubaiyat* dont ces vers immortels sont tirés :

Une coupe de vin, une miche de pain, et Toi
À mes côtés chantant dans le désert.

mais en 1070, à l'âge de 22 ans, il rédigea un ouvrage sur l'algèbre qui étudiait les solutions d'équations du troisième degré.

Le grand ouvrage mathématique de Jérôme Cardan, publié en 1545, marqua un tournant décisif dans la théorie des équations car il contenait une profusion de résultats sur les équations du troisième degré et celles du quatrième degré, qui contiennent des termes du type x^4. L'effervescence intellectuelle dans ce domaine de la recherche permit de montrer que l'on pouvait résoudre toutes les équations du deuxième, du troisième et du quatrième degré avec des formules où seules étaient utilisées les opérations $+, -, \times, \div, \sqrt[n]{\ }$ (cette dernière opération signifie la racine $n^{\text{ème}}$). On peut par exemple résoudre l'équation du second degré $ax^2 + bx + c = 0$ avec la formule :

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

L'Italian Connection

La théorie des équations du troisième degré fut entièrement développée à l'époque de la Renaissance. Malheureusement, il s'ensuivit un épisode où les mathématiques ne se montrèrent pas sous leur meilleur jour. Scipione Del Ferro trouva les solutions de l'équation du troisième degré. Informé, Niccolò Fontana, surnommé « Tartaglia » ou « Le Bègue », professeur à Venise, publia ses propres résultats sur l'algèbre sans révéler ses méthodes. Jérôme Cardan, de Milan, persuada Tartaglia de les lui révéler tout en jurant de garder le secret. Parce quelles furent divulguées malgré tout, une querelle éclata entre les deux hommes lorsque Tartaglia découvrit que son travail avait été publié en 1545 dans le livre de Cardan intitulé *Ars magna*.

1591
Dans son ouvrage mathématique, François Viète utilise des lettres pour désigner les valeurs connues et les valeurs inconnues.

Dans les années 1920
Emmy Nœther publie des articles qui ont contribué au développement de l'algèbre moderne abstraite.

1930
Bartel van der Waerden publie son célèbre *Moderne Algebra*.

Par exemple, si vous voulez résoudre l'équation $x^2 - 3x + 2 = 0$, il vous suffit d'attribuer aux paramètres les valeurs suivantes : $a = 1$, $b = -3$ et $c = 2$.

Les formules utilisées pour résoudre les équations du troisième et du quatrième degré sont longues et difficiles à manier mais elles existent bel et bien. Ce qui laissait perplexes les mathématiciens, c'est qu'ils ne savaient pas produire une formule générale qui puisse s'appliquer aux équations contenant x^5, c'est-à-dire aux équations du cinquième degré. Qu'y avait-il de si spécial avec les puissances de cinq ?

En 1826, Niels Abel, qui devait mourir prématurément, proposa une réponse remarquable pour résoudre ce casse-tête que représentaient les équations du cinquième degré. Il prouva en fait la négation d'une proposition, ce qui est souvent plus difficile que de trouver une preuve constructive. Abel prouva qu'il ne pouvait y

avoir de formule contenant les symboles +, –, ×, ÷, $\sqrt[n]{}$ pour la résolution des équations du cinquième degré, et conclut qu'il serait vain de poursuivre la quête de ce Graal. Abel réussit à convaincre les plus grands parmi les mathématiciens, mais la nouvelle mit beaucoup de temps à gagner le reste du monde mathématique. Quelques mathématiciens refusèrent d'accepter ce résultat, et pendant une bonne partie du XIXe siècle, certains continuèrent à publier des travaux pour annoncer la découverte de la formule inexistante.

Le monde moderne Pendant 500 ans, l'algèbre est resté synonyme de « théorie des équations » mais les événements prirent une nouvelle tournure au XIXe siècle. Les gens finirent par comprendre que les symboles utilisés en algèbre pouvaient représenter autre chose que des nombres. Ils pouvaient représenter des « propositions », et par conséquent l'algèbre pouvait être rattaché à l'étude de la logique. Ces symboles pouvaient même représenter des objets de dimension supérieure tels que ceux que l'on trouve dans l'algèbre des matrices (voir page 156). Et, comme de nombreux non-mathématiciens l'avaient soupçonné depuis longtemps, ils pouvaient aussi ne rien représenter du tout et n'être que des symboles régis par certaines règles, dites formelles.

Un événement capital se produisit en algèbre moderne en 1843 lorsque l'Irlandais William Rowan Hamilton découvrit les quaternions. Hamilton recherchait un système de symboles qui lui permettrait d'étendre les nombres complexes de dimension 2 à des dimensions supérieures à 2. Des années durant, il travailla sur des symboles de dimension 3, mais il n'en ressortit aucun système satisfaisant. Quand il venait déjeuner chaque matin, ses fils lui demandaient : « Alors papa, tu sais multiplier des triplets ? » et il était obligé de répondre qu'il ne savait rien faire d'autre que les additionner et les soustraire.

Le succès arriva de manière inattendue. La quête de la dimension 3 étant une impasse, il fallait se tourner vers les symboles de dimension 4. Cet éclair de génie lui est venu lors d'une promenade avec sa femme le long du Canal Royal à Dublin. La découverte le mit dans un état de pleine euphorie. Sans hésiter, le vandale de 38 ans, Astronome Royal d'Irlande et Chevalier du Royaume, grava ses formules

dans la pierre du pont Brougham, lieu marqué aujourd'hui d'une plaque pour commémorer son geste. Le souvenir de cette date ne quitta jamais Hamilton, et sa découverte devint pour lui une véritable obsession. Il en fit le sujet de ses conférences année après année et publia deux énormes volumes sur ce qu'il appela son « rêve mystique ».

Les quaternions ont une particularité : lorsqu'on les multiplie, l'ordre selon lequel on procède est d'une importance capitale, contrairement à ce qui se passe d'ordinaire en arithmétique. En 1844, le linguiste et mathématicien allemand Hermann Grassmann publia un autre système algébrique mais avec moins de brio. Ignoré à l'époque, ce système a révélé par la suite toute son ampleur. Aujourd'hui, les quaternions et l'algèbre de Grassmann ont des applications en géométrie, physique, et dans les images de synthèse.

L'abstrait Au XXe siècle, le paradigme dominant en algèbre était la méthode axiomatique. Euclide l'utilisait comme base de la géométrie, mais on l'applique en algèbre depuis relativement peu de temps.

Emmy Nœther était la championne de la méthode abstraite. Dans cette algèbre moderne, l'idée qui prévaut est l'étude de la structure où les exemples individuels sont asservis à une notion générale abstraite. Si des exemples individuels ont la même structure mais que leur notation est différente, ils sont dits isomorphes.

La structure algébrique la plus fondamentale est le groupe qui est défini par une liste d'axiomes (voir page 155). Il existe des structures comportant moins d'axiomes (tels que les monoïdes, les semi-groupes et les quasi-groupes) et des structures comportant davantage d'axiomes (tels que les anneaux, les corps gauches, les anneaux intègres et les corps). Tous ces mots nouveaux ont été introduits dans le vocabulaire mathématique au début du XXe siècle alors que l'algèbre devenait peu à peu une science abstraite connue sous le nom « d'algèbre moderne ».

l'idée clé
Méthode de résolution de l'inconnu

15 L'algorithme d'Euclide

Al-Khwarizmi nous a donné le mot « algèbre », mais c'est dans son ouvrage du IXe siècle sur l'arithmétique que le mot « algorithme » apparut pour la première fois. C'est un concept utile à la fois aux mathématiciens et aux informaticiens, mais de quoi s'agit-il ? Si nous pouvons répondre à cette question, nous sommes à deux doigts de comprendre l'algorithme d'Euclide.

D'abord, un algorithme est un programme. C'est une liste d'instructions du genre « vous faites ceci et ensuite cela ». On voit pourquoi les ordinateurs aiment les algorithmes : ils sont doués pour suivre des instructions sans jamais s'en écarter. Certains mathématiciens pensent que les algorithmes sont ennuyeux parce qu'ils sont répétitifs. Or, écrire un algorithme pour le traduire ensuite en un code informatique long de plusieurs centaines de lignes comportant des instructions mathématiques est un véritable exploit. Le risque majeur, c'est que les choses tournent horriblement mal. Écrire un algorithme est un défi créatif. Il y a souvent plusieurs méthodes possibles pour exécuter la même tâche et il faut choisir la meilleure. Quelques algorithmes ne sont parfois pas « à la hauteur » et d'autres sont parfois totalement inefficaces parce qu'ils musardent çà et là. D'autres encore sont rapides mais donnent une réponse incorrecte. C'est un peu comme la cuisine. Il doit y avoir des centaines de recettes (d'algorithmes) pour cuisiner la dinde aux marrons, et nous ne voulons pas d'un mauvais algorithme le seul jour de l'année où l'on en a réellement besoin. Nous avons donc les ingrédients ainsi que les instructions. La recette (abrégée) pourrait commencer ainsi :

- Remplissez la dinde de farce.
- Beurrez la dinde généreusement.
- Salez, poivrez, et parsemez la dinde de thym.
- Faites rôtir à 240° C pendant 3 heures et demie.
- Laissez reposer la dinde $^1/_2$ heure.

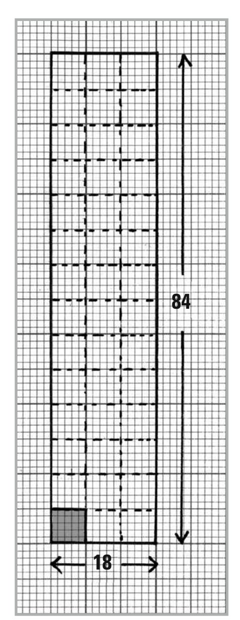
Il suffit de suivre pas à pas l'ordre séquentiel des instructions de l'algorithme. La seule chose d'ordinaire présente dans un algorithme mathématique mais qui fait

chronologie

Vers 300 av. J.-C.
L'algorithme d'Euclide est publié dans le Livre 7 des *Éléments*.

Vers l'an 300 ap. J.-C.
Sun Tzu découvre le théorème chinois.

défaut dans cette recette, c’est une boucle comme il en existe en informatique, c’est-à-dire un outil pour traiter la récursivité. Il faut espérer qu’ il ne sera pas nécessaire de cuire la dinde plus d’une fois.

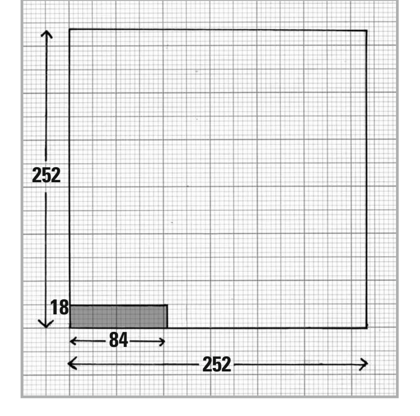


En mathématiques, il y a aussi des ingrédients : ce sont les nombres. L’algorithme d’Euclide est conçu pour calculer le plus grand diviseur commun (que l’on écrit pgcd). Le pgcd de deux entiers est le plus grand nombre qui les divise l’un et l’autre. Comme exemple, nous choisirons les deux nombres 18 et 84.

Le plus grand diviseur commun Le pgcd de notre exemple est le plus grand nombre qui divise exactement 18 et 84. Le nombre 2 divise à la fois 18 et 84, mais 3 également. Par conséquent, 6 divise aussi les deux nombres. Existe-t-il un nombre plus grand qui les divise tous deux ? Nous pourrions essayer 9 ou 18. Après vérification, ils ne sont pas des diviseurs de 84 et donc 6 est le plus grand nombre qui les divise tous les deux. On peut conclure que 6 est le pgcd de 18 et 84, et on l’écrit pgcd(18, 84) = 6.

Le pgcd peut être comparé à un carrelage de cuisine. Il correspond à la taille du plus grand carreau qui permettra de recouvrir un mur rectangulaire de 18 unités de largeur et de 84 unités de longueur, sachant qu’il est interdit de couper les carreaux utilisés. Dans cet exemple, il est clair qu’un carreau de 6 × 6 fera l’affaire.

Le plus grand diviseur commun est parfois appelé le « plus grand facteur commun ». Il est également lié à un concept voisin, celui de « plus petit multiple commun » (ppcm). Le ppcm de 18 et 84 est le plus petit nombre divisible par 18 et 84. Ce lien entre le ppcm et le pgcd est mis en évidence lorsque l’on multiplie le ppcm de deux nombres positifs par leur pgcd : le résultat obtenu est égal à celui du produit des deux nombres eux-mêmes. Ici, ppcm(18, 84) = 252, et on peut vérifier que 6 × 252 = 1 512 = 18 × 84.



Carrelage d’un carré avec des rectangles de 18 × 84

Géométriquement, le ppcm correspond à la taille du côté du plus petit carré qui peut être carrelé au moyen de carreaux rectangulaires de 18 × 84. Étant donné que ppcm(a,b) = ab/ pgcd(a,b), nous allons rechercher le pgcd. On a déjà calculé pgcd(18, 84) = 6, mais pour cela, il nous a fallu connaître les diviseurs communs de 18 et de 84. En résumé,

810
Al-Khwarizmi donne le nom « algorithme » aujourd’hui utilisé en mathématiques.

1202
Fibonacci publie un travail sur les congruences dans son *Liber Abaci*.

Dans les années 1970
Le théorème chinois est utilisé en cryptographie.

nous avons d'abord décomposé les deux nombres en produit de facteurs premiers : $18 = 2 \times 3 \times 3$ et $84 = 2 \times 2 \times 3 \times 7$. Nous avons ensuite observé que le nombre 2 leur est commun et qu'il est aussi la plus grande puissance de 2 qui les divise l'un et l'autre. En revanche, si 7 divise 84, il ne divise pourtant pas 18 et ne peut donc pas figurer dans la liste des facteurs premiers du pgcd. Nous en avons conclu que $2 \times 3 = 6$ est le plus grand nombre qui les divise tous les deux. Peut-on se dispenser de jongler ainsi avec les facteurs ? Imaginez les calculs si nous voulions trouver pgcd(17 640, 54 054). Il faudrait commencer par factoriser les deux nombres, et ce ne serait que le début. Il doit bien exister une méthode plus simple !

L'algorithme Il y a mieux en effet. L'algorithme d'Euclide apparaît dans les *Éléments*, Livre 7, Proposition 2 : « Étant donnés deux entiers positifs non premiers entre eux, trouver leur plus grand commun diviseur. »

L'algorithme d'Euclide est d'une efficacité admirable et remplace avantageusement toute cette recherche laborieuse de facteurs par une simple soustraction. Voyons comment ça marche.

Il s'agit de calculer d = pgcd(18, 84). On divise d'abord 84 par 18. La division ne tombe pas juste mais il y va 4 fois et il reste 12 :

$$84 = (4 \times 18) + 12.$$

Comme d doit être à la fois diviseur de 84 et de 18, il doit diviser le reste, à savoir 12. Par conséquent, d = pgcd(12, 18). On peut répéter le processus et diviser 18 par 12 :

$$18 = (1 \times 12) + 6.$$

Il reste alors 6, et donc d = pgcd(6, 12). En divisant 12 par 6, on a un reste de 0 de sorte que d = pgcd(0, 6). 6 est le plus grand nombre qui divise à la fois 0 et 6, et c'est donc la réponse à notre problème.

Si on calcule d = pgcd(17 640, 54 054), on a successivement 1 134, 630, 504, 126 et 0 pour restes, ce qui nous donne d = 126.

Utilisations du pgcd Le pgcd peut être utilisé dans la solution d'équations lorsque les solutions doivent nécessairement être des nombres entiers. On les appelle les équations diophantiennes, d'après le nom de l'ancien mathématicien grec Diophante d'Alexandrie.

Imaginons Marie-Chantal qui part comme chaque année passer ses vacances à la Barbade. Elle envoie Pierre, son majordome, à l'aéroport pour emmener toutes ses valises, qui pèsent chacune ou bien 18 kg ou bien 84 kg. Il lui fait savoir que le poids total à l'enregistrement était de 652 kg. Lorsqu'il revient à Monaco, Paul, le fils de Pierre, âgé de 9 ans, s'écrie soudain : « Ce n'est pas possible parce que le pgcd 6 n'est pas un diviseur de 652. » Paul laisse entendre qu'en réalité, le poids total serait plutôt de 642 kg.

Paul sait qu'il existe une solution en nombres entiers à l'équation $18x + 84y = c$ si et seulement si le pgcd 6 est un diviseur du nombre c. Il ne l'est pas pour $c = 652$ mais il l'est pour 642. Paul n'a même pas besoin de savoir combien de valises x, y des deux poids indiqués Marie-Chantal a l'intention d'emmener à la Barbade.

Le théorème chinois Lorsque le pgcd de deux nombres est égal à 1, on dit que ces nombres sont « premiers entre eux ». Ils n'ont pas besoin d'être premiers eux-mêmes mais ils doivent l'être l'un pour l'autre. Par exemple, pgcd(6, 35) = 1, même si 6 et 35 ne sont ni l'un ni l'autre des nombres premiers. Nous aurons besoin de cette définition pour le théorème chinois.

Examinons un autre problème : André ne sait pas combien il possède de bouteilles de vin, mais, lorsqu'il les range par deux, il en reste 1. Lorsqu'il les dispose en rangées de cinq dans son casier à bouteilles, il en reste 3. Combien de bouteilles a-t-il ? On sait que la division par 2 donne un reste de 1 et que la division par 5 donne un reste de 3. La première condition nous permet d'éliminer tous les nombres pairs. En examinant les nombres impairs, on trouve rapidement que 13 fait l'affaire (on peut dire sans risque d'erreur qu'André a plus de trois bouteilles, nombre qui satisfait lui aussi les conditions). Mais d'autres nombres conviendraient aussi, à savoir tous ceux qui appartiennent en fait à une suite complète qui commence ainsi : 13, 23, 33, 43, 53, 63, 73, 83…

Ajoutons maintenant une autre condition. Le nombre recherché doit donner un reste de 3 lorsqu'on le divise par 7 (les bouteilles sont arrivées par caisses de 7 et il y en avait 3 de plus). Si l'on parcourt la suite 13, 23, 33, 43, 53, 63… pour tenir compte de ce détail, on trouve que le nombre 73 fait l'affaire, mais on note que 143 aussi, tout comme 213 et tout nombre qui s'obtient en additionnant les multiples de 70 à ces nombres.

En termes mathématiques, nous avons trouvé les solutions garanties par le théorème des restes chinois, qui dit aussi que deux solutions quelconques diffèrent d'un multiple de $2 \times 5 \times 7 = 70$. Si André a entre 150 et 250 bouteilles, alors le théorème établit la solution à 213 bouteilles. Pas mal pour un théorème découvert au IIIe siècle !

l'idée clé
en route vers le plus grand

16 La logique

« S'il y a moins de voitures sur les routes, la pollution sera acceptable. Ou bien on a moins de voitures sur les routes, ou bien il faut un système de péage, ou bien encore il faut les deux à la fois. Si l'on met en place un système de péage, l'été sera vraiment trop chaud. Or, il fait plutôt frais cet été. La conclusion est inéluctable : la pollution est acceptable. »

Ce raisonnement lu dans l'éditorial d'un journal quotidien est-il « valide » ou est-il illogique ? Qu'il se tienne en tant que politique de la circulation routière ou que ce soit du journalisme de qualité nous importe peu. Ce qui nous intéresse uniquement, c'est sa validité en tant que raisonnement rationnel. La logique peut nous aider à trancher, car elle consiste à vérifier rigoureusement la solidité des raisonnements.

Deux prémisses et une conclusion Tel quel, l'extrait de journal est assez difficile à comprendre. Examinons pour commencer des raisonnements plus simples, en remontant jusqu'au philosophe grec Aristote, dit le Stagirite que l'on considère comme le fondateur de la logique. Son approche utilisait les différentes formes du syllogisme, type de raisonnement qui repose sur trois assertions : deux prémisses et une conclusion. En voici un exemple :

Tous les épagneuls sont des chiens
Tous les chiens sont des animaux

Tous les épagneuls sont des animaux

Au-dessus de la ligne, il y a les prémisses, et en dessous, la conclusion. Dans cet exemple, il y a quelque chose d'assurément incontournable dans la conclusion quel que soit le sens que l'on attribue aux mots « épagneuls », « chiens », et « animaux ». Le même syllogisme, mais avec des mots différents, s'écrit comme suit :

Toutes les pommes sont des oranges
Toutes les oranges sont des bananes

Toutes les pommes sont des bananes

chronologie

335 av. J.-C.
Aristote formalise la logique du syllogisme.

1847 ap. J.-C.
Boole publie *Analyse mathématique de la logique*.

Dans cet exemple, chaque assertion est complètement absurde si l'on utilise les mots dans leur sens habituel. Pourtant, ces deux exemples de syllogisme ont la même structure, et c'est cette structure qui fait que le syllogisme est valide. Il est tout simplement impossible de trouver un exemple avec ce type de structure où les prémisses A et B seraient justes mais la conclusion C fausse. C'est ce qui fait qu'un raisonnement valide est utile.

Différents types de syllogismes sont possibles si l'on utilise des quantificateurs variés tels que « tous », « certains », et « aucun » (comme dans « Aucun A n'est B »). On pourrait par exemple écrire cet autre syllogisme :

Certains A sont B
Certains B sont C

Certains A sont C

Tous les A sont des B
Tous les B sont des C

Tous les A sont des C

Un raisonnement valide

Cet argument est-il valide ? S'applique-t-il à tous les cas de A, B, et C sans exception, ou y-a-t-il un contre-exemple quelque part, un exemple où les prémisses sont vraies mais la conclusion fausse ? Et si l'on prenait des épagneuls pour A, des objets marron pour B, et des tables pour C ? L'exemple suivant est-il convaincant ?

Certains épagneuls sont marron
Certains objets marron sont des tables

Certains épagneuls sont des tables

Notre contre-exemple montre que ce syllogisme n'est absolument pas valide. Il y avait un si grand nombre de types différents de syllogismes que les savants du Moyen-Âge inventèrent des procédés mnémotechniques pour les mémoriser. Notre premier exemple appartient au mode dit B**A**RB**A**R**A** parce qu'il contient trois propositions universelles **A**ffirmatives du type « tous les ». Ces méthodes d'analyse des raisonnements ont été utilisées pendant plus de 2 000 ans et ont occupé une place de choix dans les premières années d'études universitaires à l'époque médiévale. La logique, ou théorie des syllogismes d'Aristote, a été considérée comme une science parfaite pendant une bonne partie du XIXe siècle.

Logique propositionnelle Un autre type de logique va plus loin que les syllogismes. Elle traite de propositions ou d'affirmations simples et de leurs combinaisons entre elles. Pour analyser l'éditorial, il nous faut quelques connaissances sur cette « logique propositionnelle ». On l'appelait autrefois « algèbre de la logique », ce qui nous donne un indice sur sa structure, car George Boole s'était rendu compte que l'on pouvait la considérer comme une nouvelle sorte d'algèbre. Dans les années

1910
Russell et Whitehead tentent de réduire les mathématiques à de la logique.

1965
Lofti Zadeh développe la logique floue.

1987
Au Japon, le métro est conduit par un ordinateur qui fonctionne en logique floue.

1840, un gros travail fut réalisé dans ce domaine par des mathématiciens tels que Boole et Augustus de Morgan.

a	b	a ∨ b
V	V	V
V	F	V
F	V	V
F	F	F

Table de vérité du « ou »

Faisons l'essai avec une proposition **a**, où **a** représente la proposition « Franck est un épagneul ». La proposition **a** peut être vraie ou fausse. Si je pense à mon chien qui s'appelle Franck et qui est aussi un épagneul, alors la proposition est vraie **(V)**, mais si je pense que cette proposition s'applique à mon cousin dont le nom est également Franck, alors la proposition est fausse **(F)**. La vérité d'une proposition dépend de ce à quoi elle fait référence.

a	b	a ∧ b
V	V	V
V	F	F
F	V	F
F	F	F

Table de vérité du « et »

Si nous avons une autre proposition notée **b** telle que « Esther est un chat », alors on peut combiner ces deux propositions de plusieurs manières. L'une de ces combinaisons peut s'écrire sous la forme **a** ∨ **b**. Le connecteur logique ∨ correspond à « ou » dont la signification en logique diffère légèrement de celle de notre « ou » de tous les jours. En logique, **a** ∨ **b** est vraie si l'on a ou bien « Fred est un épagneul » est vraie, ou bien « Esther est un chat » est vraie, ou bien si les deux propositions sont vraies ; elle est fausse uniquement lorsque les deux propositions **a** et **b** sont fausses. Cette conjonction de propositions peut se résumer dans une table de vérité.

a	¬b
V	F
F	V

Table de vérité de la négation

On peut aussi combiner des propositions avec « et », que l'on écrit sous la forme **a** ∧ **b**, ainsi qu'avec « non « que l'on écrit ¬**a**. L'algèbre de la logique devient limpide lorsque l'on combine ces propositions avec ces différents connecteurs logiques comme suit : **a** ∧ (**b** ∨ **c**). On obtient une relation que l'on appelle une identité :

$$\mathbf{a} \wedge (\mathbf{b} \vee \mathbf{c}) \equiv (\mathbf{a} \wedge \mathbf{b}) \vee (\mathbf{a} \wedge \mathbf{c})$$

a	b	a ⇒ b
V	V	V
V	F	F
F	V	F
F	F	F

Table de vérité de « l'implication »

Le symbole ≡ signifie qu'il y a équivalence entre les affirmations logiques, les deux côtés de l'identité ayant la même table de vérité. On peut établir un parallèle entre l'algèbre de la logique et l'algèbre ordinaire parce que les symboles ∧ et ∨ jouent le même rôle que × et + en algèbre ordinaire, où l'on a $x \times (y + z) = (x \times y) + (x \times z)$. Le parallèle n'est cependant pas total car il y a des exceptions.

D'autres connexions logiques peuvent être définies à l'aide de connecteurs élémentaires de ce genre. Un connecteur bien utile est celui de « l'implication » **a** ⇒ **b**, qui est équivalent à ¬**a** ∨ **b** et dont la table de vérité est représentée ci-contre.

Si l'on reprend maintenant l'éditorial, on peut l'écrire sous forme symbolique :

V ⇒ P V ∨ P S ⇒ C ¬C
P

V = moins de **V**oitures sur les routes
P = la **P**ollution sera acceptable
S = il faut un **S**ystème de péage
C = l'été sera vraiment trop **C**haud

Le raisonnement est-il valide ou non ? Supposons que la conclusion **P** soit fausse mais que les prémisses soient vraies. Si l'on peut montrer qu'il y a contradiction, cela signifie que le raisonnement est certainement valide. Il sera donc impossible que les prémisses soient vraies mais la conclusion fausse. Si **P** est fausse, alors d'après la première prémisse $\mathbf{V} \Rightarrow \mathbf{P}$, **V** doit être fausse. Comme $\mathbf{V} \vee \mathbf{S}$ est vraie, le fait que **V** soit fausse signifie que **S** est vraie. De la troisième prémisse $\mathbf{S} \Rightarrow \mathbf{C}$, on déduit que **C** est vraie. Autrement dit, $\neg\mathbf{C}$ est fausse. Cela contredit le fait que $\neg\mathbf{C}$, la dernière prémisse, puisse être supposée vraie. Le contenu des assertions de l'éditorial peut toujours être contesté, mais la structure du raisonnement est valide.

D'autres logiques Gottlob Frege, C.S. Peirce et Ernst Schröder introduisirent la quantification dans la logique propositionnelle pour construire « une logique des prédicats du premier ordre » (parce qu'elle est fondée sur des variables). Elle utilise le quantificateur universel ∀, pour signifier « quel que soit », et le quantificateur existentiel ∃, pour dire « il existe ».

∨	ou
∧	et
¬	n'est pas
⇒	implique
∀	quel que soit
∃	il existe

Une idée nouvelle est apparue en logique : la logique floue. On imagine une pensée confuse, mais elle a permis au contraire un élargissement des frontières traditionnelles de la logique. La logique traditionnelle repose sur des ensembles. Ainsi, nous avons eu l'ensemble des épagneuls, l'ensemble des chiens, et l'ensemble des objets marron. Nous savons de manière certaine ce qui est inclus dans l'ensemble et ce qui ne l'est pas. Si nous croisons un rottweiler pure race dans le parc, nous pouvons être sûrs qu'il n'appartient pas à l'ensemble des épagneuls.

La théorie des ensembles flous traite de ce qui apparaît comme des ensembles définis de manière imprécise. Et si l'on avait l'ensemble des gros épagneuls ? Combien doit peser un épagneul pour appartenir à cet ensemble ? Avec les ensembles flous, il y a une gradation de l'appartenance, tandis que la frontière qui sépare ce qui est dans l'ensemble de ce qui ne l'est pas reste floue. Les mathématiques nous autorisent à être précis en ce qui concerne le flou. La logique est loin d'être une matière austère. Elle a évolué depuis Aristote et constitue aujourd'hui un domaine actif de la recherche moderne et de ses applications.

l'idée clé
Le cheminement clair de la pensée

17 Les preuves

Les mathématiciens essaient de justifier leurs affirmations en apportant des preuves. La recherche d'arguments rationnels irréfutables est le moteur des mathématiques pures. Des enchaînements de déductions correctes tirées de ce qui est connu ou supposé conduisent le mathématicien à une conclusion qui vient alors prendre place parmi tous les produits mathématiques dûment certifiés.

Il n'est pas facile d'établir des preuves. On les atteint souvent au terme d'un gros travail d'exploration qui parfois nous entraîne sur de fausses pistes. Les efforts déployés pour apporter ces preuves occupent l'essentiel de la vie du mathématicien. Une preuve réussie porte l'estampille de ce dernier, et fait accéder la conjecture, qui n'est rien d'autre qu'une idée géniale ou une simple supposition, au statut de théorème.

Les qualités recherchées dans une preuve sont la rigueur, la limpidité mais également l'élégance. À cela s'ajoute l'ingéniosité. Une bonne preuve est « une preuve qui aiguise notre esprit de discernement », mais il est aussi préférable d'avoir une preuve quelle qu'elle soit que de ne pas en avoir du tout. En effet, avec une progression qui repose sur des faits non prouvés, on court le risque de construire les théories sur l'équivalent mathématique des sables mouvants.

Non pas qu'une preuve soit éternelle. Il faut parfois la réviser à la lumière des nouveaux développements des concepts auxquels elle se rattache.

Qu'est-ce qu'une preuve ? Lorsque vous lisez ou entendez parler d'un résultat mathématique, le croyez-vous ? Qu'est-ce qui pourrait vous inciter à lui accorder crédit ? On pourrait répondre que ce serait un argument solide d'un point de vue logique qui part des idées que vous acceptez pour aller jusqu'à la proposition sur laquelle vous vous interrogez. Ce serait ce que les mathématiciens appellent une preuve, qui a la particularité de généralement mêler langage courant et logique stricte. Selon la qualité de la preuve, ou bien vous êtes convaincu, ou bien vous demeurez sceptique.

Les principaux types de preuves que l'on utilise en mathématiques sont : la méthode du contre-exemple, la méthode directe, la méthode indirecte et le raisonnement par récurrence.

chronologie

Vers 300 av. J.-C.
Les *Éléments* d'Euclide fournissent le modèle des preuves mathématiques.

1637 ap. J.-C.
Descartes présente la rigueur mathématique comme un modèle à suivre dans son *Discours de la méthode.*

Le contre-exemple Commençons par faire preuve de scepticisme, méthode qui consiste à prouver qu'une proposition est incorrecte. Prenons un exemple concret. Supposons que l'on vous dise que tout nombre multiplié par lui-même donne un nombre pair. Le croyez-vous ? Avant de nous précipiter pour répondre, il faudrait faire quelques essais. Si nous prenons un nombre quelconque, 6 par exemple, et que nous le multiplions par lui-même, ce qui donne $6 \times 6 = 36$, on trouve que le résultat est bien un nombre pair. Mais une hirondelle ne fait pas le printemps. L'énoncé stipule que la proposition est vraie pour tout nombre, et il y en a une infinité. Pour bien faire, il faudrait essayer avec d'autres exemples. Si l'on prend 9, par exemple, on trouve $9 \times 9 = 81$, et 81 est un nombre impair. Cela signifie que la proposition selon laquelle tout nombre multiplié par lui-même donne un nombre pair est fausse. Un tel exemple va à l'encontre de l'hypothèse de départ et s'appelle un contre-exemple. Un contre-exemple à la proposition « tous les cygnes sont blancs » serait un cygne noir. Une partie de l'amusement que procurent les mathématiques tient dans la recherche d'un contre-exemple qui viendrait démolir un prétendu théorème.

Si l'on ne parvient pas à trouver de contre-exemple, on peut avoir l'impression que la proposition est correcte. Il faut alors que le mathématicien change son fusil d'épaule. Une preuve doit nécessairement être construite et, si l'on veut aller droit au but, on utilise la méthode directe.

La méthode directe Avec la méthode directe, on s'appuie sur une argumentation logique qui découle de ce qui a déjà été établi, ou de ce qui est supposé vrai, pour progresser vers la conclusion. Si l'on y parvient, on a un théorème. Il est impossible de prouver que la multiplication d'un nombre quelconque par lui-même donne un nombre pair parce que nous avons déjà prouvé que c'était faux. Mais nous sommes peut-être capables de conserver quelque chose de cet énoncé. La différence entre notre premier exemple, 6, et le contre-exemple 9, est que le premier nombre est pair et que celui du contre-exemple est impair. Changer l'hypothèse est possible. Notre proposition est donc maintenant : si l'on multiplie un nombre pair par lui-même, le résultat est un nombre pair.

On commence par tester quelques autres exemples numériques. Cette proposition se vérifie à chaque fois et il est absolument impossible de trouver un contre-exemple. On change de tactique pour tenter de le prouver, mais comment faut-il s'y prendre ? On pourrait d'abord prendre un nombre pair quelconque noté n, mais comme c'est un peu trop abstrait, nous verrons comment une preuve peut être établie à partir d'un nombre concret, par exemple 6. Comme vous le savez, un nombre pair est un multiple de 2. Ainsi, $6 = 2 \times 3$. Étant donné que $6 \times 6 = 6 + 6 + 6 + 6 + 6 + 6$, ou d'une autre façon, $6 \times 6 = 2 \times 3 + 2 \times 3 + 2 \times 3 + 2 \times 3 + 2 \times 3 + 2 \times 3$ ou encore, avec des parenthèses,

$$6 \times 6 = 2 \times (3 + 3 + 3 + 3 + 3 + 3)$$

1838
De Morgan introduit le terme « récurrence ».

1967
Bishop prouve des résultats en utilisant exclusivement des méthodes constructives.

1976
Imre Lakatos publie un ouvrage de référence intitulé *Preuves et réfutations*.

cela signifie que 6×6 est un multiple de 2, et que c'est donc un nombre pair. Mais ce raisonnement peut s'appliquer à d'autres nombres que 6. Ainsi, nous aurions pu commencer avec $n = 2 \times k$ pour obtenir

$$n \times n = n \times 2 \times k = 2 \times n \times k = 2 \times (k + k + \ldots + k)$$

et conclure que $n \times n$ est pair. Notre preuve est maintenant complète. Autrefois, les mathématiciens comme Euclide utilisaient la formule « QED » à la fin d'une preuve pour dire que la démonstration était faite. C'est une abréviation qui signifie en latin *quod erat demonstrandum* (ce qui devait être démontré). De nos jours, ils utilisent un carré □ (■ autrefois). C'est ce que l'on appelle parfois un halmos, du nom de Paul Halmos qui l'a introduit.

La méthode indirecte Avec cette méthode, on prétend que la conclusion est fausse et, à l'aide d'un raisonnement logique, on démontre que cela contredit l'hypothèse. Prouvons le résultat précédent en suivant cette méthode.

Notre hypothèse est que n est pair et nous prétendrons que $n \times n$ est impair. On peut écrire $n \times n = n + n + \ldots + n$, n fois. Cela signifie que n ne peut pas être pair, parce que s'il l'était, $n \times n$ serait pair. Donc n est impair, ce qui contredit l'hypothèse. □

Ce que l'on vient de voir est en fait une version douce de la méthode indirecte. La version dure de cette méthode, connue sous le nom de *reductio ad absurdum* (raisonnement par l'absurde), était très appréciée des Grecs. À l'Académie d'Athènes, Socrate et Platon aimaient prouver un point litigieux en enveloppant leurs opposants dans les filets de la contradiction pour qu'il ne reste au final que l'argument qu'ils essayaient de prouver. La preuve classique que la racine carrée de 2 est un nombre irrationnel relève de cette méthode. On suppose d'abord que la racine carrée de 2 est un nombre rationnel et c'est de là que découle une contradiction à l'hypothèse de départ.

Le raisonnement par récurrence (ou induction mathématique) La récurrence est une façon efficace de démontrer que des assertions successives $P1$, $P2$, $P3$, … sont vraies. C'est ce qu'Augustus De Morgan a admis dans les années 1830 lorsqu'il a formalisé ce qui était connu depuis plusieurs centaines d'années. Cette technique spécifique (qui ne doit pas être confondue avec l'induction utilisée dans les sciences expérimentales) est largement utilisée pour prouver des propositions qui contiennent des nombres entiers naturels. Elle est particulièrement utile dans la théorie des graphes, la théorie des nombres, et de manière générale, en informatique. Pour prendre un exemple concret, pensez au problème de l'addition des nombres impairs. L'addition des trois premiers nombres impairs $1 + 3 + 5$ donne 9 alors que la somme des quatre premiers $1 + 3 + 5 + 7$ donne 16. Mais 9 est égal à $3 \times 3 = 3^2$ et 16 est égal à $4 \times 4 = 4^2$. Se pourrait-il donc que la somme des n premiers nombres impairs soit égale à n^2 ? Si nous essayons avec une valeur de n choisie de manière aléatoire, par exemple $n = 7$, on trouve en effet que la somme des sept premiers nombres impairs est égale à $1 + 3 + 5 + 7 + 9 + 11 + 13 = 49$, ou 7^2. Mais est-ce un schéma suivi par toutes les valeurs de n ? Il y a problème, car nous ne pouvons espérer pouvoir vérifier individuellement un nombre infini de cas.

C'est ici qu'intervient la récurrence. Pour parler simplement, c'est la méthode des dominos. Cette métaphore s'applique à des dominos posés debout les uns derrière les autres. Si un domino tombe, il renversera son voisin. C'est évident. Tout ce dont nous avons besoin pour les faire tous tomber, c'est que le premier tombe. On peut appliquer cette manière de penser au problème des nombres impairs. L'assertion *P*n dit que la somme des n premiers nombres impairs est égale à n^2. La récurrence mathématique produit une réaction en chaîne par laquelle P_1, P_2, P_3, … seront toutes vraies. La proposition P_1 est évidemment vraie parce que $1 = 2^2$. Ensuite, P_2 est vraie parce que $1 + 3 = 1^2 + 3 = 2^2$, P_3 est vraie parce que $1 + 3 + 5 = 2^2 + 5 = 3^2$ et P_4 est vraie parce que $1 + 3 + 5 + 7 = 3^2 + 7 = 4^2$. On utilise un résultat pour passer au suivant. Ce processus peut être formalisé pour encadrer la méthode de récurrence mathématique.

Les difficultés des preuves Les preuves se présentent dans toutes sortes de styles et de tailles. Certaines sont courtes et efficaces, comme celles que l'on trouve dans les manuels. D'autres, qui exposent les toutes dernières recherches dans leurs moindres détails, font l'objet d'un traitement spécifique dans des revues qui leur consacrent des milliers de pages. Très peu de gens peuvent alors se faire une idée du raisonnement complet.

De plus, certains fondements posent parfois problème. Par exemple, un petit nombre de mathématiciens ne sont pas satisfaits de la méthode de raisonnement par l'absurde lorsqu'il s'agit de prouver l'existence. Si la proposition selon laquelle il n'y a pas de solution à une équation conduit à une contradiction, est-ce suffisant pour prouver qu'une solution existe ? Les détracteurs de cette méthode affirmeraient que cette logique n'est qu'un tour de passe-passe et ne nous dit pas comment construire vraiment une solution concrète. Les « Constructivistes », qui appartiennent à plusieurs courants, sont les mathématiciens qui stipulent que la méthode utilisée dans la preuve ne donne pas « une signification numérique ». Ils couvrent de mépris les mathématiciens classiques qui considèrent la méthode de récurrence comme une arme essentielle dans l'arsenal mathématique. D'un autre côté, les mathématiciens les plus traditionnels diraient que proscrire ce type de raisonnement revient à se priver d'un outil bien utile, et, de plus, que rejeter tant de résultats prouvés au moyen de cette méthode indirecte ne laisserait plus que la trame de la tapisserie mathématique.

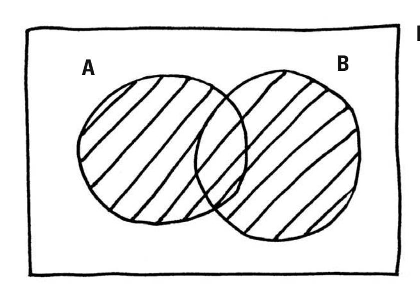


18 Les ensembles

Nicolas Bourbaki était le pseudonyme que s'était donné un groupe fermé d'universitaires français qui voulaient récrire les mathématiques « comme il faut », à partir de la base. Dans leur audace, ils déclaraient que la théorie des ensembles devait constituer le fondement des mathématiques. Adeptes de la méthode axiomatique, ils publièrent des livres rédigés dans un style rigoureux émaillé de « définitions, théorèmes et preuves ». C'était aussi l'époque de l'envolée du mouvement des mathématiques modernes des années 1960.

Georg Cantor créa la théorie des ensembles pour donner des bases saines à la théorie des nombres réels. Initialement controversée et critiquée, la théorie des ensembles fut malgré tout reconnue comme une branche des mathématiques dès le début du XXe siècle.

Qu'est-ce qu'un ensemble ? On peut considérer qu'un ensemble est une collection d'objets. C'est une définition simple qui nous donne cependant l'idée essentielle. Les objets sont eux-mêmes appelés les « éléments » de l'ensemble. Si l'on écrit un ensemble A qui contient un élément a, on peut noter $a \in A$ comme le faisait Cantor. Voici un autre exemple : $A = \{1, 2, 3, 4, 5\}$. On peut écrire $1 \in A$ pour noter l'appartenance, et $6 \notin A$ pour indiquer la non-appartenance.



Union de A et B

Les ensembles peuvent être essentiellement combinés de deux manières. Si A et B sont deux ensembles, alors l'ensemble qui comprend des éléments appartenant à A ou à B (ou bien aux deux) s'appelle « l'union » $\cup$ des deux ensembles. Les mathématiciens l'écrivent sous la forme $A \cup B$. Il peut aussi être représenté sous la forme d'un diagramme de Venn (ou « patate »), baptisé ainsi d'après le Révérend John Venn, grand logicien de l'époque victorienne. Euler utilisait déjà des diagrammes de ce genre des années plus tôt.

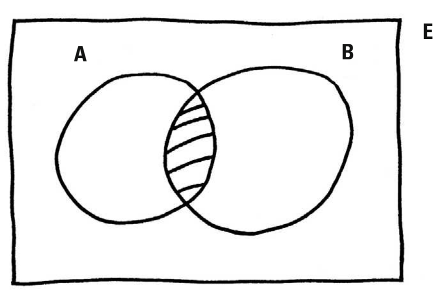
L'ensemble $A \cap B$ est constitué des éléments qui appartiennent à la fois à A et à B. On l'appelle « l'intersection » des deux ensembles.

chronologie

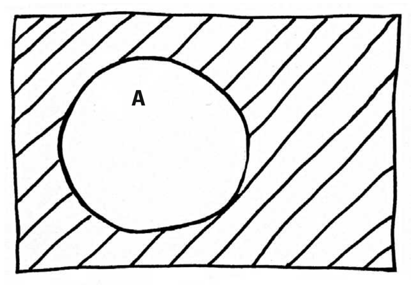
1872
Cantor fait une petite avancée vers la création d'une théorie des ensembles.

1881
Venn popularise « les diagrammes de Venn » pour représenter les ensembles.

Si $A = \{1, 2, 3, 4, 5\}$ et $B = \{1, 3, 5, 7, 10, 21\}$, l'union des deux ensembles s'écrit $A \cup B = \{1, 2, 3, 4, 5, 7, 10, 21\}$ et leur intersection $A \cap B = \{1, 3, 5\}$. Si l'on considère qu'un ensemble A fait partie d'un ensemble universel E, on peut définir l'ensemble complémentaire $\neg A$ comme l'ensemble des éléments de E qui n'appartiennent pas à A.



Intersection de A et de B



Complément de A

Les opérations $\cap$ et $\cup$ sur des ensembles fonctionnent de manière analogue aux opérations $\times$ et + en algèbre. Si on leur ajoute l'opération complémentaire $\neg$, on peut dire qu'il y a une « algèbre des ensembles ». Augustus De Morgan, mathématicien britannique né en Inde, formula des lois pour montrer le fonctionnement de toutes ces opérations. Rédigées dans notre notation moderne, les lois de De Morgan s'écrivent ainsi :

$$\neg(A \cup B) = (\neg A) \cap (\neg B)$$

et

$$\neg(A \cap B) = (\neg A) \cup (\neg B)$$

Les paradoxes Il n'existe pas de problèmes portant sur les ensembles finis parce que l'on peut dénombrer leurs éléments. Ainsi, $A = \{1, 2, 3, 4, 5\}$. Mais à l'époque de Cantor, les ensembles infinis représentaient eux une véritable gageure.

Cantor définit les ensembles comme un groupe d'éléments dotés d'une propriété spécifique. Pensez à l'ensemble {11, 12, 13, 14, 15…}, de tous les nombres entiers strictement supérieurs à 10. Parce que l'ensemble est infini, on ne peut pas dénombrer tous ses éléments, mais il nous est toujours possible de définir cet ensemble grâce à la propriété que partagent tous ses éléments. À l'instar de Cantor, on peut écrire l'ensemble sous la forme $A = \{x \mid x$ est un nombre entier $> 10\}$, où la barre signifie « tel que ».

Initialement, dans la théorie des ensembles, on pouvait aussi avoir un ensemble de choses abstraites tel que $A = \{x \mid x$ est une chose abstraite$\}$. Dans ce cas, A est lui-même une chose abstraite, c'est pourquoi on peut avoir $A \in A$. Mais l'autorisation de cette relation fait surgir de sérieux problèmes. Le philosophe et mathématicien britannique Bertrand Russell eut l'idée d'un ensemble S qui contiendrait toutes les choses qui ne se contiennent pas elles-mêmes. En notation symbolique, on l'écrit $S = \{x \mid x \notin x\}$.

1931
Gödel prouve que tout système axiomatique mathématique formel contient des affirmations indécidables.

1939
Le pseudonyme Bourbaki est utilisé pour la première fois.

1964
Cohen prouve l'indépendance de l'hypothèse du continu.

Il demanda ensuite : « Est-ce que $S \in S$? » Si la réponse est « Oui », alors S doit satisfaire la définition de S, et donc $S \notin S$. D'un autre côté, si la réponse est «Non » et que $S \notin S$, alors S ne satisfait pas la relation qui définit S, à savoir $S \notin S$, et donc $S \in S$. Le problème de Russell se terminait par cette proposition, qui est à la base du paradoxe de Russell.

$$S \in S \text{ si et seulement si } S \notin S.$$

C'est un problème semblable au « paradoxe du barbier », où un barbier annonce aux gens de son village qu'il ne rasera que ceux qui ne se rasent pas eux-mêmes. La question qui se pose est alors de savoir si le barbier doit se raser lui-même. S'il ne se rase pas lui-même, alors oui, il le doit. S'il se rase lui-même, alors il ne le doit pas.

Il est impératif d'éviter de tels paradoxes, que l'on appelle poliment des « antinomies ». Pour les mathématiciens, on ne peut tout simplement pas autoriser des systèmes qui génèrent des contradictions. Russell créa une théorie des types qui n'autorise la relation $a \in A$ que si a est d'un type strictement inférieur à A, ce qui permet ainsi d'éviter des relations telles que $S \in S$.

Une autre manière d'éviter ces antinomies était de formaliser la théorie des ensembles. Dans cette approche, on ne se préoccupe pas de la nature des ensembles eux-mêmes, mais on dresse la liste d'axiomes formels qui précisent les règles qui les régissent. Les Grecs ont expérimenté quelque chose d'analogue avec un problème qui les intéressait : expliquer ce qu'étaient les droites n'était pas nécessaire, il suffisait de savoir ce que l'on pouvait en faire.

Dans le cas de la théorie des ensembles, ce sont les axiomes de la théorie des ensembles de Zermelo-Fraenkel qui empêchèrent l'apparition d'ensembles trop « gros » pour le système auquel ils appartenaient. C'était un moyen efficace d'interdire l'apparition d'une créature aussi dangereuse que l'ensemble de tous les ensembles.

Le théorème de Gödel Le mathématicien autrichien Kurt Gödel anéantit les espoirs de tous ceux qui se réfugiaient dans les systèmes axiomatiques formels pour tenter d'échapper aux paradoxes. En 1931, Gödel prouva que même le plus simple des systèmes formels contenait des énoncés dont on ne pouvait dire de l'intérieur de ce même système s'ils étaient vrais ou non. Plus simplement, il s'agissait d'énoncés qui échappaient aux axiomes du système auxquels ils appartenaient. C'étaient des énoncés indécidables. On appelle pour cette raison le théorème de Gödel « le théorème de l'incomplétude ». Ce résultat s'appliquait au système de Zermelo-Fraenkel ainsi qu'à d'autres.

Les nombres cardinaux Le nombre d'éléments d'un ensemble fini est facile à trouver, par exemple $A = \{1, 2, 3, 4, 5\}$ comporte 5 éléments, ou bien on dit que son cardinal est égale à 5, ce qui s'écrit card $A = 5$. En gros, le cardinal est la mesure de la « taille » d'un ensemble.

Selon la théorie des ensembles de Cantor, l'ensemble des fractions $\mathbf{Q}$ et celui des nombres réels $\mathbf{R}$ sont très différents. L'ensemble $\mathbf{Q}$ est dénombrable alors que

l'ensemble **R** ne l'est pas (voir page 31). Tous deux sont infinis, mais l'ensemble **R** a un plus grand ordre d'infinité que **Q**. Les mathématiciens indiquent le card **Q** par $\aleph_0$, « l'aleph 0 » hébreux, et card **R** = *c*. Cela signifie donc que $\aleph_0 < c$.

L'hypothèse du continu Mise en lumière par Cantor en 1878, l'hypothèse du continu stipule que le niveau suivant d'infinité après l'infinité de **Q** est l'infinité des nombres réels *c*. En d'autres termes, selon l'hypothèse du continu, il n'existe pas d'ensemble dont le cardinal est strictement compris entre $\aleph_0$ et *c*. Malgré tous ses efforts et bien que persuadé de la véracité de cette hypothèse, Cantor n'a pas réussi à en apporter la preuve. La réfuter revient à trouver un sous-ensemble *X* de **R** avec $\aleph_0 < \text{card } X < c$, mais il ne parvint pas à trouver un tel ensemble non plus.

Le problème était si difficile que le mathématicien David Hilbert le plaça en tête de la célèbre liste de 23 problèmes ouverts lancée à l'adresse des chercheurs du siècle suivant, liste qu'il présenta au Congrès mathématique international de Paris en 1900.

Gödel était absolument convaincu que l'hypothèse était fausse mais il n'en apporta pas la preuve. Il réussit à prouver (en 1938) que l'hypothèse était compatible avec les axiomes de la théorie des ensembles de Zermelo-Fraenkel. Un quart de siècle plus tard, Paul Cohen stupéfia Gödel et les logiciens en prouvant que l'hypothèse du continu ne pouvait se déduire des axiomes de Zermelo-Fraenkel. Cela revient à montrer que l'on peut avoir à la fois les axiomes et l'hypothèse du continu ou sa négation, si la théorie des ensembles est non contradictoire. Ce résultat, combiné avec celui de Gödel trouvé en 1938, permit à Cohen de montrer que l'hypothèse du continu était indépendante des axiomes de la théorie des ensembles.

Cette conclusion est à rapprocher de la manière dont il y a indépendance du postulat des parallèles (ou postulat d'Euclide) en géométrie (voir page 108) et des autres axiomes d'Euclide. Cette découverte entraîna une floraison de géométries non euclidiennes, qui, entre autres choses, permirent l'avancée de la théorie de la relativité d'Einstein. De la même manière, l'hypothèse du continu peut être acceptée ou rejetée sans gêner les autres axiomes de la théorie des ensembles. Après le résultat novateur trouvé par Cohen, c'est un domaine entier qui fut créé. Il attira des générations de mathématiciens qui adoptèrent les techniques utilisées pour prouver l'indépendance de l'hypothèse du continu.

l'idée clé
Une multitude traitée comme un élément unique

19 Le calcul différentiel

Il y a différents types de calculs, et les mathématiciens parlent donc parfois du « calcul de la logique », du « calcul des probabilités », et ainsi de suite. Mais ils sont tous d'accord pour dire qu'il n'existe purement et simplement qu'un seul Calcul, le calcul différentiel, et qu'il s'écrit avec un C majuscule.

Le Calcul différentiel est un élément capital des mathématiques. Il serait aujourd'hui impossible qu'un scientifique, un ingénieur ou un spécialiste de l'économie quantitative n'ait jamais eu affaire au Calcul différentiel, si larges sont ses applications. Historiquement, il est associé à Isaac Newton et Gottfried Leibniz qui en furent les instigateurs au XVIIe siècle. Leurs théories très proches les amenèrent à s'opposer dans une querelle de priorité pour savoir qui avait découvert le Calcul différentiel en premier. En fait, les deux hommes aboutirent à la même conclusion indépendamment l'un de l'autre en suivant des méthodes assez différentes.

Depuis lors, le Calcul différentiel a pris une importance colossale. Chaque génération ne jure que par certaines techniques que, selon elle, la nouvelle génération devrait apprendre, et c'est ainsi que de nos jours, les manuels, régulièrement complétés, dépassent le millier de pages. Malgré tous ces ajouts, les points essentiels sont la « différentiation » (ou « dérivation ») et « l'intégration », qui se partagent toutes les deux la vedette dans le Calcul différentiel tel que Newton et Leibniz l'ont défini. Ces termes viennent de « *differentialis* » (prendre les différences ou « séparer ») et « *integralis* » (faire la somme des parties ou « mettre ensemble »), mots utilisés par Leibniz.

En langage technique, la dérivation est chargée de mesurer le *changement*, et l'intégration de mesurer *l'aire*, mais la cerise sur le gâteau du Calcul différentiel est ce « résultat phare » selon lequel dérivation et intégration sont les deux facettes du même problème : elles sont l'inverse l'une de l'autre. Le Calcul différentiel forme véritablement un tout dont il est nécessaire de connaître les deux faces. Il n'est pas étonnant que le modèle parfait du Major Général moderne imaginé en 1879 par

chronologie

Vers 450 av. J.-C.
Zénon discrédite le calcul infinitésimal au moyen d'un paradoxe.

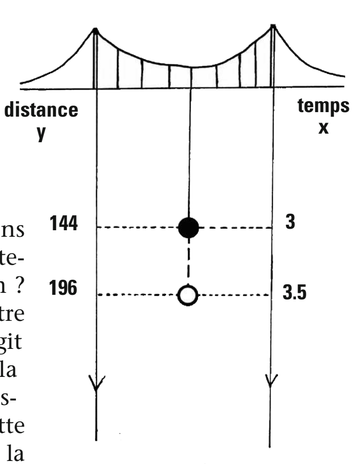
1660–1670 ap. J.-C.
Newton et Leibniz sont les pionniers du Calcul différentiel.

Gilbert et Sullivan dans l'opérette *The Pirates of Penzance* se vante de les maîtriser toutes les deux :

Mon savoir sur le carré de l'hypoténuse est démentiel,
Et je suis un as du calcul intégral et différentiel.

Différentiation Les scientifiques, et Einstein tout particulièrement, adorent conduire des « expériences de pensée ». Imaginez que nous sommes sur un pont au-dessus d'une gorge profonde et que nous nous apprêtons à jeter une pierre. Que va-t-il se passer ? Par la pensée, on peut aussi faire des choses impossibles comme arrêter la pierre dans sa chute ou la regarder tomber au ralenti pendant un court moment. Nul besoin de notre présence physique !

Selon la théorie de la gravitation de Newton, la pierre va tomber. Rien de surprenant ici : la pierre subit l'attraction terrestre et tombera de plus en plus vite à mesure de l'avancée de l'aiguille sur notre chronomètre. Un autre avantage de ces expériences par la pensée, c'est que l'on peut ignorer des facteurs qui viennent compliquer les choses, comme par exemple la résistance de l'air.



Quelle est la vitesse de la pierre à un instant donné, disons lorsque l'aiguille du chronomètre indique 3 secondes exactement après le top de départ ? Comment trouver la solution ? On peut certainement mesurer la vitesse moyenne mais notre problème est de mesurer la vitesse instantanée. Comme il s'agit d'une expérience par la pensée, pourquoi ne pas arrêter la pierre dans sa chute puis la laisser tomber sur une courte distance en ajoutant une fraction de seconde ? Si l'on divise cette distance supplémentaire par le temps additionnel, on aura la vitesse moyenne pendant ce court intervalle de temps. En prenant des intervalles de temps de plus en plus courts, la vitesse moyenne sera de plus en plus proche de la vitesse instantanée à l'endroit où nous avons arrêté la pierre.

Nous pourrions être tentés de prendre un temps additionnel égal à zéro. Mais dans notre expérience par la pensée, la pierre ne bouge pas du tout. Elle parcourt une distance nulle en un temps nul ! Cela nous donnerait la vitesse moyenne 0/0 que le célèbre évêque philosophe irlandais Berkeley décrivait comme « les fantômes de quantités disparues ». Une telle vitesse ne peut pas être déterminée : elle est en fait dépourvue de sens. En prenant cette voie, nous allons tout droit dans un bourbier numérique.

1734
Berkeley attire l'attention sur les faiblesses des fondements du Calcul différentiel.

Dans les années 1820
Cauchy formalise la théorie avec rigueur.

1854
Riemann introduit l'intégrale de Riemann.

1902
Lebesgue établit la théorie de l'intégrale de Lebesgue.

Pour aller plus loin, il nous faut quelques symboles. La formule exacte qui relie la distance y parcourue lors de la chute au temps x nécessaire pour atteindre un point donné a été trouvée par Galilée :

$$y = 16 \times x^2.$$

Le facteur « 16 » apparaît parce que pieds et secondes sont les unités de mesure choisies. Si l'on veut savoir, par exemple, quelle distance la pierre aura parcouru en 3 secondes, il suffit de remplacer x par 3 dans la formule et de calculer la réponse : $y = 16 \times 3^2 = 144$ pieds (43,9 mètres). Mais comment calculer la vitesse de la pierre au moment $x = 3$?

Prenons une demi-seconde de plus et voyons la distance parcourue par la pierre entre 3 et 3,5 secondes. En 3,5 secondes, la pierre parcourt $y = 16 \times 3{,}5^2 = 196$ pieds (59,7 m), et donc entre 3 et 3,5 secondes elle parcourt 196 – 144 = 52 pieds (15,8 m). Comme la vitesse est égale à la distance divisée par le temps, la vitesse moyenne pendant cet intervalle de temps est égale à 52/0,5 = 104 pieds (31,7 m) par seconde. Ce résultat sera plus proche de la vitesse instantanée de la pierre après 3 secondes de chute (lorsque $x = 3$).

Il faut maintenant prendre le taureau par les cornes et traiter le problème du calcul de la vitesse moyenne de la pierre entre x secondes et légèrement plus tard à $x + h$ secondes. Après une petite manipulation on trouve :

$$16 \times (2x) + 16 \times h.$$

Étant donné que l'on réduit h graduellement, comme nous l'avons fait en passant de 0,5 à 0,05, on voit que le premier terme n'est pas affecté (parce qu'il ne contient pas h) et que le second terme lui-même devient de plus en plus petit. On en conclut que

$$v = 16 \times (2x)$$

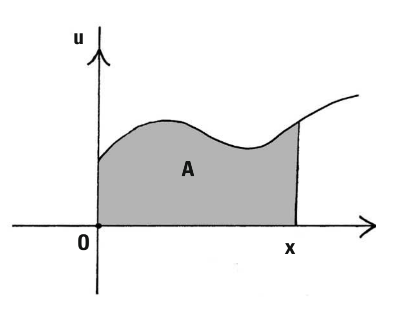
où v est la vitesse instantanée de la pierre au moment x. La vitesse instantanée de la pierre après 1 seconde (quand $x = 1$) par exemple est égale à $16 \times (2 \times 1) = 32$ pieds (9,7 m) par seconde ; après 3 secondes, elle est égale à $16 \times (2 \times 3)$, ce qui donne 96 pieds (29,3 m) par seconde.

u	du/dx
x^2	$2x$
x^3	$3x^2$
x^4	$4x^3$
x^5	$5x^4$
...	...
x^n	nx^{n-1}

Si l'on compare la formule de la distance de Galilée $y = 16 \times x^2$ avec la formule de la vitesse $v = 16 \times (2x)$, la différence essentielle tient dans le changement de x^2 en $2x$. L'effet de la dérivation, c'est ce passage de $u = x^2$ à la dérivée $u. = 2x$. Newton appelait $u. = 2x$ une « fluxion » et la variable x un « fluent » parce qu'il pensait en termes de quantités fluides. De nos jours, on écrit fréquemment $u = x^2$ et sa dérivée $du/dx = 2x$. Initialement introduite par Leibniz, l'utilisation de cette notation aujourd'hui encore témoigne de la supériorité du formalisme de Leibniz sur celui de Newton.

La pierre qui tombe était un exemple, mais si u représentait autre chose, on pourrait toujours calculer la dérivée, ce qui peut être utile dans d'autres contextes. Il existe

un procédé pour obtenir la dérivée des fonctions x^n : on diminue de 1 la puissance de x et on multiplie le tout par n.



Intégration La première application de l'intégration a concerné la mesure des aires. La mesure d'une aire sous une courbe s'obtient en la divisant en bandes rectangulaires de largeur dx. On mesure les aires de tous les rectangles et l'on additionne ensuite ces aires pour trouver leur « somme » et donc l'aire approximative totale. La notation de S sous la forme allongée $\int$ pour désigner cette somme a été introduite par Leibniz. L'aire de chacune des bandes rectangulaires est égale à u dx, et donc l'aire A sous la courbe de 0 à x est égale à

$$A = \int_0^x u \, \mathrm{d}x$$

Si la courbe que nous étudions est $u = x^2$, on trouve l'aire en traçant des rectangles très étroits sous la courbe, on additionne leurs aires pour calculer l'aire approximative, puis on calcule la limite de la somme des aires des rectangles lorsque leur largeur tend vers 0 pour obtenir l'aire exacte. Cette réponse donne

$$A = x^3/3.$$

On peut toujours, pour des courbes différentes, et donc pour d'autres expressions de u, calculer l'intégrale. Comme la dérivée, il existe un procédé pour calculer l'intégrale des fonctions x^n. Elle s'obtient en augmentant de 1 la puissance de x et en divisant le tout par ce nouvel exposant.

u	$A = \int_0^x u dx$
x^2	$x^3/3$
x^3	$x^4/4$
x^4	$x^5/5$
x^5	$x^6/6$
...	...
x^n	$x^{n+1}/(n+1)$

Le résultat phare Si l'on dérive l'intégrale $A = x^3/3$, on retrouve le résultat initial $u = x^2$. Si l'on intègre la dérivée du/dx = 2x, on obtient aussi le résultat initial $u = x^2$. La dérivation est l'opération inverse de l'intégration, observation connue sous le nom de « théorème fondamental du calcul différentiel », qui est aussi l'un des théorèmes les plus importants de toutes les mathématiques.

Sans le Calcul différentiel, il n'y aurait pas de satellites en orbite, pas de théorie économique et les statistiques seraient une discipline complètement différente de ce qu'elles sont. Là où il se produit du changement, on trouve le Calcul différentiel.

l'idée clé
Tendre vers la limite

20 Les constructions

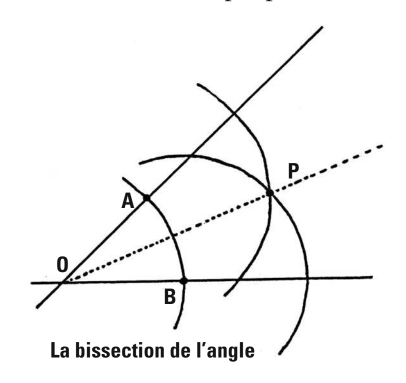
Prouver une négation est souvent difficile, mais certains triomphes mathématiques ne font rien d'autre. Cela signifie que l'on prouve que quelque chose est impossible. La quadrature du cercle est impossible, mais comment en apporter la preuve ?

Les Grecs de l'Antiquité avaient quatre grands problèmes de géométrie à résoudre :

- la trisection de l'angle (diviser un angle en trois angles égaux plus petits),
- la duplication du cube (construire un second cube dont le volume est le double de celui du premier cube),
- la quadrature du cercle (créer un carré dont l'aire est égale à celle d'un cercle donné),
- la construction de polygones (construire des formes régulières dont les côtés et les angles sont égaux).

Pour mener à bien ces tâches, ils n'utilisaient que le strict minimum :

- une règle pour tracer des droites (et certainement pas pour mesurer des longueurs),
- un compas pour tracer des cercles.



La bissection de l'angle

Si vous êtes adepte de l'escalade en montagne sans corde, sans oxygène, sans téléphone portable et tout autre équipement encombrant, ces problèmes vont très certainement vous plaire. Privées du matériel moderne de mesure que nous connaissons, les techniques mathématiques avaient besoin de prouver que leurs résultats étaient tout de même sophistiqués. Ce n'est d'ailleurs qu'au XIXe siècle que les problèmes classiques de géométrie ont été résolus grâce aux techniques de l'analyse moderne et de l'algèbre abstraite.

La trisection de l'angle Voici une façon de diviser un angle en deux angles égaux plus petits, ou,

chronologie

450 av. J.-C
Anaxagore tente de réaliser la quadrature du cercle alors qu'il est en prison.

1672 ap. J.-C.
Mohr montre que toutes les constructions euclidiennes peuvent être réalisées au compas seul.

en d'autres termes, d'en faire la bissection. Placez d'abord la pointe du compas sur le point 0, et, en prenant un rayon quelconque, notez OA et OB. Placez la pointe du compas sur A et tracez un arc de cercle. Procédez de même avec B. Notez P le point d'intersection des arcs de cercle, et joignez O et P à la règle. Les triangles AOP et BOP sont semblables et donc les angles AOP et BOP sont égaux. La droite (OP) est la bissectrice recherchée puisqu'elle coupe l'angle en deux angles égaux.

Pouvons-nous suivre une procédure semblable pour couper un angle quelconque en trois angles égaux ? C'est le problème de la trisection de l'angle.

Si l'angle est de 90°, c'est donc un angle droit, et il n'y a pas de problème parce que l'on peut construire un angle de 30°. Mais, si l'on prend un angle de 60° par exemple, on ne peut absolument pas faire la trisection de cet angle. On sait que la réponse est 20° mais il n'existe aucune manière de construire un tel angle à la règle et au compas. Donc, pour résumer :

- on peut toujours faire la bissection d'un angle.
- on peut faire la trisection de certains angles ayant des valeurs particulières, mais
- on ne peut jamais faire la trisection d'un angle quelconque.

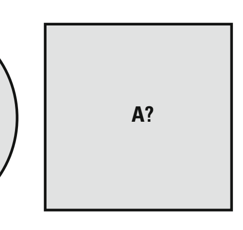
La duplication du cube est un problème similaire que l'on appelle le problème déliaque ou de Délos. On raconte que les habitants de Délos en Grèce consultèrent l'oracle au sujet de la peste qui sévissait alors. Il leur recommanda de construire un nouvel autel, dont le volume serait le double de celui de l'autel déjà existant.

Imaginez l'autel de Délos comme un cube dont tous les côtés sont de longueur *a*. Il leur fallait donc construire un autre cube de longueur *b* ayant deux fois le volume du premier. Le volume de chacun des cubes est égal à a^3 et b^3 et ils sont donc liés par l'équation $b^3 = 2a^3$, ce qui donne $b = a\sqrt[3]{2}$, où 3$\sqrt[3]{2}$ est le nombre qui, multiplié par lui-même trois fois, donne 2 (la racine cubique). Si le côté du cube initial est $a = 1$, les habitants de Délos devaient noter la longueur $\sqrt[3]{2}$ sur une droite. Malheureusement pour eux, c'est une tâche impossible à effectuer à la règle et au compas quelle que soit l'ingéniosité déployée pour réaliser la construction souhaitée.

La quadrature du cercle Ce problème est légèrement différent mais c'est aussi le plus connu de tous les problèmes de géométrie :

Construire un carré dont l'aire est égale à l'aire d'un cercle donné.

A



La quadrature du cercle

1801
Gauss publie *Recherches arithmétiques* qui comprend une partie consacrée à la construction d'un polygone à 17 côtés à la règle et au compas.

1837
Wantzel prouve que les problèmes classiques de duplication d'un cube ou de trisection d'un angle ne peuvent pas se résoudre à la règle et au compas.

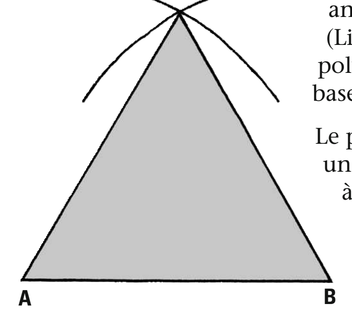
1882
Lindemann prouve que la quadrature du cercle est impossible.

L'expression « la quadrature du cercle » est communément utilisée pour désigner l'impossible. L'équation algébrique $x^2 - 2 = 0$ a pour solutions $x = \sqrt{2}$ et $x = -\sqrt{2}$. Ce sont des nombres irrationnels (on ne peut pas les écrire sous forme de fractions), mais montrer que la quadrature du cercle est impossible revient à montrer que π ne peut pas être solution d'une équation algébrique. Les nombres irrationnels qui ont cette propriété sont appelés des nombres transcendants parce que leur irrationalité est « plus élevée » que celle de leurs cousins irrationnels de la forme $\sqrt{2}$.

Les mathématiciens croyaient généralement que π était un nombre transcendant mais cette « énigme éternelle » restait difficile à prouver jusqu'au jour où Ferdinand von Lindemann se servit, en l'adaptant, d'une technique mise au point par Charles Hermite. Hermite l'avait utilisée pour prouver que la base des logarithmes naturels, *e*, était transcendante, problème plus facile à résoudre (voir page 26).

Après le résultat de Lindemann, on aurait pu penser que tarirait enfin le flot d'articles publiés par ces irréductibles « spécialistes de la quadrature du cercle ». Pas du tout. Il y avait toujours dans les coulisses des mathématiques de joyeux drilles qui rechignaient à accepter la logique de la preuve et d'autres qui n'avaient jamais entendu parler d'elle.

Construction de polygones Euclide posa le problème de la construction d'un polygone régulier. Il s'agit d'une figure symétrique à plusieurs côtés, comme un carré ou un pentagone, dont tous les côtés sont de longueur égale et dont les côtés adjacents délimitent des angles égaux entre eux. Dans son ouvrage célèbre, les *Éléments* (Livre 4), Euclide a montré comment on pouvait construire des polygones à 3, 4, 5, et 6 côtés à l'aide de nos deux seuls outils de base, la règle et le compas.



La construction d'un triangle équilatéral

Le polygone à 3 côtés est ce que nous appelons communément un triangle équilatéral, figure qui est particulièrement simple à construire. Quelle que soit la taille du triangle que vous voulez construire, notez un point A et un point B séparés par la distance souhaitée. Placez la pointe du compas sur le point A et dessinez une partie du cercle de rayon AB. Répétez le processus en plaçant la pointe du compas sur le point B et en conservant le même rayon. Le point d'intersection de ces deux arcs de cercle se trouve en P. Comme AP = AB et BP = AB, alors les trois côtés du triangle APB sont égaux. Le triangle peut être tracé en joignant AB, AP et BP à la règle.

Si vous pensez que travailler avec une règle est un luxe, vous n'êtes pas le seul : le danois Georg Mohr le pensait aussi. Le triangle équilatéral se construit à partir du point P et, pour ce faire, seul le compas est nécessaire. La règle ne sert qu'à relier physiquement les points entre eux. Mohr a montré que toute construction réalisable à la règle et au compas peut se réaliser au compas seul. L'Italien Lorenzo Mascheroni prouva le même résultat 125 ans plus tard. Toute l'originalité de son

livre *Géometrie du compas* qu'il écrivit en 1797 et dédié à Napoléon, tient à sa rédaction en vers.

Pour le cas général, les polygones à p côtés où p est un nombre premier sont particulièrement importants. Nous avons déjà construit le polygone à 3 côtés, et Euclide construisit le polygone à 5 côtés, mais il ne parvint pas à construire de polygone à 7 côtés (l'heptagone). Étudiant le problème à l'âge de 17 ans, un certain Carl Friederich Gauss prouva la négation. Il prouva par déduction qu'il n'est pas possible de construire un polygone à p côtés pour $p = 7$, 11, ou 13.

Mais Gauss prouva également une proposition positive, à savoir qu'il est possible de construire un polygone à 17 côtés. En réalité, il alla bien plus loin en prouvant que l'on peut construire un polygone à p côtés si et seulement si le nombre premier p est de la forme

$$p = 2^{2^n} + 1.$$

Les nombres de cette forme sont appelés les nombres de Fermat. Si l'on effectue les calculs pour $n = 0$, 1, 2, 3 et 4, on obtient les nombres premiers $p = 3$, 5, 17, 257 et 65 537, qui correspondent à des polygones à p côtés que l'on peut construire.

Lorsque l'on essaie $n = 5$, le nombre de Fermat est $p = 2^{32} + 1 = 4\,294\,967\,297$. Pierre de Fermat conjectura qu'ils étaient tous des nombres premiers, mais malheureusement, celui-ci n'en est pas un, parce que $4\,294\,967\,297 = 641 \times 6\,700\,417$. Si l'on prend $n = 6$ ou 7, les résultats sont des nombres de Fermat gigantesques, mais, comme avec $n = 5$, aucun n'est premier.

Y a-t-il d'autres nombres premiers de Fermat ? Il est prudent de dire que non, mais personne ne le sait de façon certaine.

Naissance d'un prince

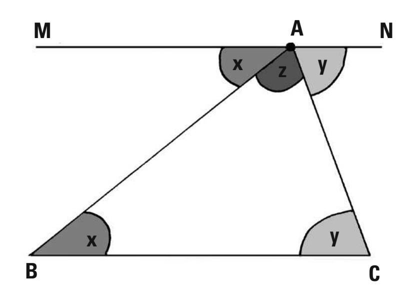
Carl Friedrich fut si impressionné d'avoir réussi à prouver que l'on peut construire un polygone à 17 côtés qu'il décida de mettre un terme à ses études de langues et de devenir mathématicien. Le reste appartient à l'histoire : on le surnomma le « prince des mathématiques ». La forme du polygone à 17 côtés a été choisie pour construire la base de son mémorial à Göttingen en Allemagne, hommage digne de son génie.

l'idée clé

Prenez une règle et un compas…

21 Les triangles

De toute évidence, un triangle est une figure à trois côtés qui comporte trois angles (tri-angles). La trigonométrie est la théorie que l'on utilise pour « mesurer les triangles », que ce soit la taille de leurs angles, la longueur de leurs côtés, ou leur aire. Cette forme, l'une des plus simples de toutes les figures, présente un intérêt qui ne s'est jamais démenti.



Le conte du triangle Il existe un joli petit raisonnement pour montrer que la somme des angles d'un triangle quelconque donne deux angles droits, soit un angle de 180°. Tracez une droite (MN) qui passe par le point ou « sommet » A d'un triangle quelconque et qui est parallèle à la base [BC].

L'angle ABC, que nous appelons x, est égal à l'angle BAM parce que ce sont des angles alternes-internes et que (MN) et (BC) sont parallèles. Les deux autres angles alternes-internes sont égaux à y. L'angle au point A est de 180° (la moitié de 360°) et c'est $x + y + z$ qui est égal à la somme des angles du triangle. QED, comme l'écrivait jadis Euclide en conclusion de ses preuves. Bien sûr, nous supposons que l'angle est tracé sur une surface plane comme cette feuille de papier. La somme des angles d'un triangle tracé sur un ballon (un triangle sphérique) n'est pas égale à 180°, mais c'est une tout autre histoire.

Euclide prouva de nombreux problèmes sur les triangles mais toujours au moyen d'un raisonnement par déduction. Il montra par exemple que « la somme des longueurs des deux côtés d'un triangle quelconque est supérieure ou égale à la longueur du troisième côté ». C'est ce que l'on appelle aujourd'hui « l'inégalité triangulaire », inégalité importante en mathématiques. Les Épicuriens, avec leur approche matérialiste de la vie, affirmaient qu'aucune preuve n'était requise car c'était une évidence même pour un âne. Si l'on plaçait une balle de foin à un sommet et que l'âne se tenait à un autre sommet, disaient-ils, l'animal ne remonterait sûrement pas les deux côtés pour apaiser sa faim.

Le théorème de Pythagore Le plus grand théorème concernant les triangles est le théorème de Pythagore. Il est aujourd'hui incontournable, même si l'on ne sait pas vraiment si Pythagore fut bien le premier à le découvrir. C'est en termes

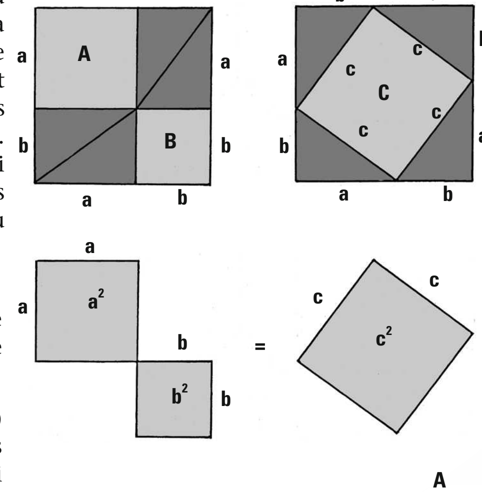
chronologie

1850 av. J.-C.
Les Babyloniens connaissent le théorème de Pythagore.

1335 ap. J.-C.
Richard de Wallingford écrit un traité innovant sur la trigonométrie.

algébriques qu'il est le mieux formulé : $a^2 + b^2 = c^2$. Mais dans la version géométrique du théorème, Euclide fait référence à de véritables carrés : « Aux triangles rectangles, le carré du côté qui soutient l'angle droit, est égal aux carrés des deux autres côtés. »

La preuve d'Euclide, qui correspond à la Proposition 47, Livre 1 des *Éléments*, est par la suite devenue un véritable sujet d'inquiétude pour des générations d'écoliers qui redoublaient d'efforts pour l'apprendre par cœur et ne pas avoir à subir les conséquences de leur ignorance. Il en existe des centaines de preuves. Celle qui remporte tous les suffrages est plus proche, dans l'esprit, d'une preuve découverte par Bhaskara au XIIe siècle que de la preuve fournie par Euclide, qui remonte à 300 ans av. J.-C.



C'est une preuve « sans parole ». Sur notre figure, le carré de côté $a + b$ peut être divisé de deux manières différentes.

Puisque les quatre triangles égaux (en noir) sont communs aux deux carrés, on peut les enlever tout en conservant l'égalité d'aire. Si l'on examine les aires des figures restantes, la formule bien connue jaillit soudain :

$$a^2 + b^2 = c^2.$$

La droite d'Euler On peut formuler des centaines de propositions sur les triangles. Prenons d'abord les points des milieux des côtés. Dans un triangle ABC quelconque, on note D, E, F les points des milieux des trois côtés. Reliez les points B et F puis C et D et notez G le point d'intersection où les droites se coupent. Reliez à présent A et E. Cette droite passe-t-elle également par le point G ? Il n'est pas évident de le savoir sans pousser plus avant le raisonnement. En réalité, elle passe effectivement par le point G qui s'appelle le « centre de gravité » du triangle.

Il existe littéralement des centaines de « centres » différents dans un triangle. On connaît par exemple le point H où se coupent les hauteurs (les droites passant par les sommets et perpendiculaires aux côtés opposés, en pointillés sur la figure page 86). C'est « l'orthocentre ». Il en existe aussi un autre qui s'appelle le « centre du cercle circonscrit » O où chacune des droites (appelées « médiatrices ») se rencontrent en D, E et F (non représentées). C'est le centre du cercle qui passe par A, B et C.

1571
François Viète publie un livre sur la trigonométrie et des tables trigonométriques.

1822
Karl Feuerbach découvre le cercle des 9 points d'un triangle.

1873
Brocard présente un travail très complet sur le triangle.

Mais il y a mieux. Dans tout triangle ABC, les points G, H et O, qui sont respectivement le centre de gravité, l'orthocentre et le centre du cercle circonscrit, sont eux-mêmes alignés sur une droite appelée « la droite d'Euler ». Dans le cas d'un triangle équilatéral (où les trois côtés sont de même longueur), ces trois points se confondent en un point qui est de toute évidence le centre du triangle.

La droite d'Euler

Le théorème de Napoléon Si pour un triangle ABC quelconque, on construit un triangle équilatéral sur chacun de ses trois côtés, les centres de gravité de ces triangles forment un nouveau triangle DEF. Le théorème de Napoléon stipule que pour tout triangle ABC, le triangle DEF est un triangle équilatéral.

Ce théorème a été publié pour la première fois dans un journal anglais en 1825, quelques années après la mort de Napoléon à Sainte-Hélène en 1821. Les capacités de Napoléon en mathématiques l'ont sans nul doute aidé à obtenir son admission à l'école de guerre, et plus tard, devenu empereur, il rencontra les mathématiciens de Paris les plus en vue. Malheureusement, aucune preuve ne peut nous permettre d'en dire plus et le « théorème de Napoléon » est, comme beaucoup d'autres résultats mathématiques, attribué à une personne qui a peu à voir avec sa découverte ou sa preuve. C'est en effet un théorème qui est constamment redécouvert et élargi.

Le théorème de Napoléon

Les données essentielles qui déterminent un triangle sont la longueur d'un côté et la mesure de deux angles. En utilisant la trigonométrie, on peut mesurer tout le reste.

Lorsque l'on fait un levé topographique de territoires pour dresser des cartes, il est plutôt utile de se comporter comme ces « Flatlanders » qui habitent le pays plat imaginé par Edwin E. Abbot et donc de supposer que les triangles sont plats. On établit un réseau de triangles à partir d'une base [BC] de longueur connue. On choisit ensuite un point A extérieur à cette base (le point de triangulation) et on mesure les angles ABC et ACB avec un théodolite. Grâce à la trigonométrie, on sait tout du triangle ABC, et le géomètre peut ainsi progresser et placer le point de triangulation suivant en fonction de la nouvelle position des bases [AB] ou [AC] et répéter l'opération pour constituer un maillage de triangles. La méthode permet de dresser les cartes d'endroits inhospitaliers qui comportent des obstacles tels que des marécages, des tourbières, des sables mouvants et des fleuves.

C'est ce qui a servi de base pour effectuer le grand relevé trigonométrique de l'Inde commencé dans les années 1800 et qui s'acheva 40 ans plus tard. L'objectif était de faire un levé topographique afin d'établir la carte de la région du grand Arc Méridien, depuis Cap Comorin dans le sud, jusqu'à l'Himalaya au nord, sur une distance d'environ 2500 kilomètres. Pour garantir la plus grande précision dans la mesure des angles, Sir George Everest fit fabriquer deux théodolites géants à Londres de 1 tonne

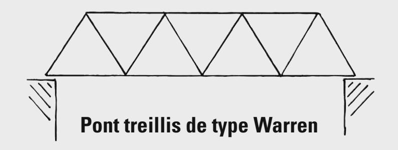
chacun et que seules des équipes d'une douzaine d'hommes étaient capables de transporter. Il était essentiel d'avoir des mesures d'angle exactes. Le problème de la précision des mesures était au cœur des conversations, mais c'était l'humble triangle qui était au centre des opérations. Les Victoriens devaient se débrouiller sans GPS même s'ils disposaient déjà d'ordinateurs, mais il s'agissait d'ordinateurs humains. Dès que toutes les longueurs d'un triangle sont calculées, il est facile de trouver son aire. Une fois encore, le triangle est l'unité. Il existe plusieurs formules pour calculer l'aire A d'un triangle, mais la plus remarquable est celle de Héron d'Alexandrie :

$$A = \sqrt{p \times (p-a) \times (p-b) \times (p-c)}$$

où p désigne le demi-périmètre du triangle dont les côtés sont de longueur a, b, et c. On peut l'appliquer à tous les triangles et il n'est même pas nécessaire de connaître la mesure des angles. Si un triangle a des côtés de 13, 14 et 15 par exemple, son périmètre est égal à $13 + 14 + 15 = 42$, et donc $p = 21$. Pour terminer le calcul, $A = \sqrt{(21 \times 8 \times 7 \times 6)} = \sqrt{7056}$ $= 84$. Le triangle est un objet familier, que ce soit pour les enfants qui jouent avec des formes simples, ou pour les chercheurs en mathématiques qui utilisent jour après jour l'inégalité triangulaire. La trigonométrie est le fondement des calculs sur les triangles, et les fonctions sinus, cosinus et tangente sont les outils utilisés pour les décrire, car elles permettent les calculs précis dont on a besoin pour des applications pratiques. Le triangle a fait l'objet d'une attention soutenue, mais il est surprenant qu'il reste tant à découvrir sur les trois droites qui forment cette figure si élémentaire.

Construire avec des triangles

Le triangle est incontournable en construction. Très utilisé, il tient toute sa force de cette propriété qui en fait un élément indispensable pour effectuer des levés de terrain : il est rigide. On peut déformer un carré ou un rectangle mais pas un triangle. La ferme de toit utilisée en construction est un assemblage de triangles jugé essentiel. Cette structure trouva une application inattendue dans la construction de ponts. Une ferme de type Warren peut accepter une lourde charge comparée à son poids. James Warren la fit breveter en 1848 et deux ans plus tard, le premier pont conçu selon ce principe était construit à la gare London Bridge de Londres. Il s'avère que cette structure, qui est constituée de triangles équilatéraux, est plus solide que ces autres structures constituées de triangles isocèles, triangles dont deux côtés seulement sont égaux.



Pont treillis de type Warren

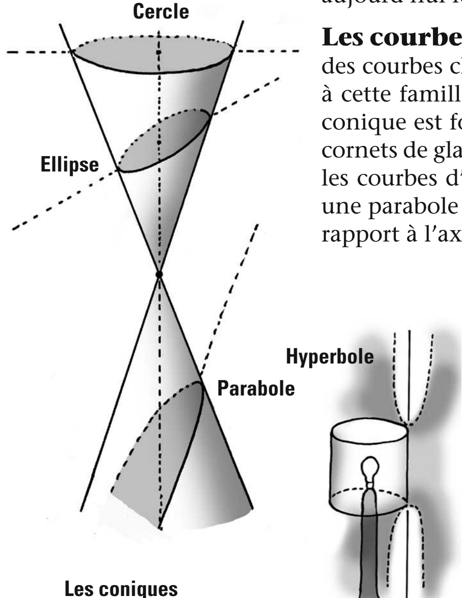
l'idée clé
Les trois angles d'un même problème

22 Les courbes

Il est facile de tracer une courbe. Les artistes le font tout le temps ; les architectes conçoivent de larges hémicycles de bâtiments neufs qui épousent la courbe d'une rue ou d'un quartier pavillonnaire. Au base-ball, les lanceurs envoient des balles en leur donnant de l'effet. Les footballeurs remontent le terrain en suivant une courbe, et lorsqu'ils tirent au but, la trajectoire de la balle dessine une courbe. Mais si d'aventure nous posions la question, « qu'est-ce qu'une courbe ? », la réponse ne serait pas si simple à formuler.

Les mathématiciens étudient les courbes depuis des siècles en prenant des points de vue différents. Tout a commencé avec les Grecs qui étudiaient ce que l'on appelle aujourd'hui les courbes « classiques ».





Les coniques

Les courbes classiques La première famille dans le monde des courbes classiques s'appelle « les coniques ». Appartiennent à cette famille le cercle, l'ellipse, la parabole et l'hyperbole. La conique est formée à partir d'un double cône, réunion de deux cornets de glace dont l'un est à l'envers. Si un plan coupe le tout, les courbes d'intersection obtenues sont un cercle, une ellipse, une parabole ou une hyperbole, selon l'inclinaison du plan par rapport à l'axe vertical du cône.

On peut imaginer une conique comme la projection d'un cercle sur un écran. Les rayons de lumière émis par l'ampoule d'une lampe cylindrique forment un cône double de lumière où se projettent les bords circulaires supérieurs et inférieurs de la lampe. L'image projetée au plafond est un cercle, mais si l'on penche la lampe, ce cercle devient une ellipse. D'un autre côté, l'image projetée sur le mur reproduit la courbe en deux parties, autrement dit sous forme d'une hyperbole.

Les coniques peuvent aussi être décrites en fonction du déplacement de points dans le plan.

chronologie

Vers 300 av. J.-C.
Euclide définit les coniques.

Vers 250 av. J.-C.
Archimède étudie les spirales.

Vers 225 av. J.-C.
Apollonius de Perge publie *Éléments des coniques.*

C'est la méthode du « lieu géométrique » chère aux Grecs, et qui, contrairement à la définition projective, nécessite des indications de longueur. Si un point se déplace et que la distance qui le sépare d'un autre point unique fixe reste la même, on a un cercle. Si un point se déplace et que la somme des distances qui le sépare de deux points fixes (« les foyers ») est une valeur constante, on obtient une ellipse (lorsque les foyers sont les mêmes, l'ellipse devient un cercle). L'ellipse fut la clé pour comprendre le déplacement des planètes. En 1609, l'astronome allemand Johannes Kepler proclama que les planètes tournent autour du Soleil selon des trajectoires elliptiques, rejetant ainsi la vieille idée d'orbites circulaires.

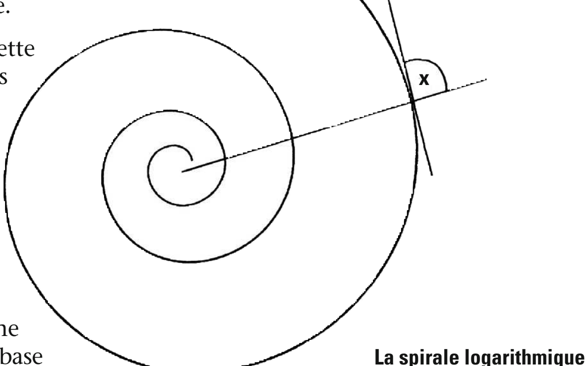
Moins évident : le point qui se déplace de telle façon que sa distance par rapport à un point (le foyer F) est la même que la distance qui le sépare perpendiculairement d'une droite donnée (la directrice). Dans ce cas, on obtient une parabole. La parabole possède un tas de propriétés utiles. Si une source de lumière est placée au foyer F, les rayons de lumière émis sont parallèles à [PM]. D'un autre côté, si des signaux envoyés par un satellite viennent frapper une parabole réceptrice, ils convergent vers le foyer pour être ensuite dirigés vers le téléviseur.

M
P
F

La parabole

Si l'on fait tourner une baguette autour d'un point, tous les points fixes de la baguette dessinent un cercle, mais si un point se déplace le long de la baguette et tourne avec cette baguette, on obtient une spirale. Les Pythagoriciens aimaient beaucoup les spirales et, bien des années plus tard, Léonard de Vinci passa dix ans de sa vie à en étudier les différents types ; quant à René Descartes, il écrivit un traité à leur sujet. La spirale logarithmique s'appelle aussi la spirale équiangle parce que l'angle délimité par un rayon et la tangente est constant quel que soit le point où le rayon rencontre la spirale.

Jacob Bernoulli, qui appartenait à cette illustre famille de mathématiciens suisses, était si épris de la spirale logarithmique qu'il la fit graver sur sa tombe à Bâle. « L'homme de la Renaissance » Emmanuel Swedenborg considérait la spirale comme la forme la plus parfaite de toutes. Une spirale à trois dimensions qui s'enroule autour d'un cylindre s'appelle une hélice. Deux hélices (une double hélice) forment la structure de base de l'ADN.



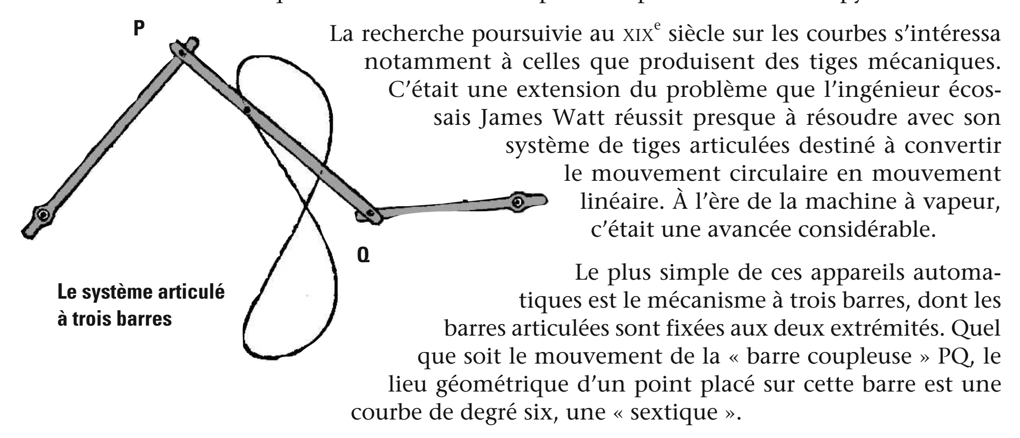
La spirale logarithmique

1704 ap. J.-C.
Newton classifie les courbes cubiques.

1890
Peano prouve qu'un carré plein est une courbe (la courbe de Peano).

Dans les années 1920
Menger et Urysohn définissent les courbes comme appartenant au domaine de la topologie.

Il existe un grand nombre de courbes classiques, telles que le limaçon, la lemniscate et les divers ovales. La cardioïde s'appelle ainsi parce qu'elle est en forme de cœur. La courbe caténaire fit l'objet de recherches au XVIII[e] siècle et fut identifiée comme la courbe dessinée par une chaînette qui pend entre deux points. La caténaire est cette courbe que l'on observe dans les ponts suspendus entre deux pylônes.



Le système articulé à trois barres

La recherche poursuivie au XIX[e] siècle sur les courbes s'intéressa notamment à celles que produisent des tiges mécaniques. C'était une extension du problème que l'ingénieur écossais James Watt réussit presque à résoudre avec son système de tiges articulées destiné à convertir le mouvement circulaire en mouvement linéaire. À l'ère de la machine à vapeur, c'était une avancée considérable.

Le plus simple de ces appareils automatiques est le mécanisme à trois barres, dont les barres articulées sont fixées aux deux extrémités. Quel que soit le mouvement de la « barre coupleuse » PQ, le lieu géométrique d'un point placé sur cette barre est une courbe de degré six, une « sextique ».

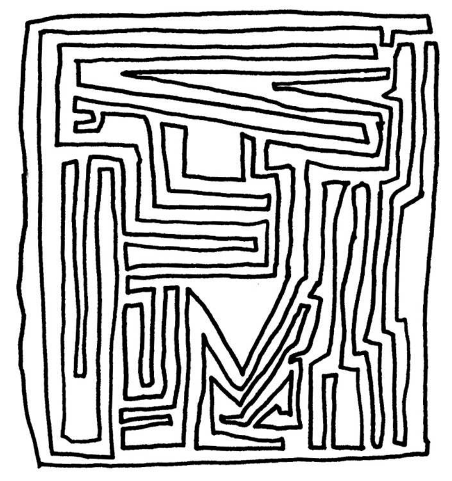
Les courbes algébriques Après Descartes, qui révolutionna la géométrie avec l'introduction des coordonnées x et y et les axes cartésiens auxquels il donna son nom, les coniques pouvaient maintenant être étudiées à l'aide d'équations algébriques. Le cercle centré en l'origine et de rayon 1 a par exemple pour équation $x^2 + y^2 = 1$, qui est une équation du second degré, et il en est ainsi pour toutes les coniques. Une nouvelle branche de la géométrie appelée géométrie analytique se développa alors.

Dans une étude capitale, Isaac Newton classifia les courbes qui s'écrivent sous la forme d'équations algébriques de degré trois, ou courbes cubiques. Aux quatre coniques de base, il opposa 78 types différents de cubiques qu'il regroupa en cinq classes. Le nombre de types différents de quartiques est en pleine expansion, mais il y en a tellement que la classification reste inachevée à ce jour.

L'histoire ne s'arrête pas avec l'étude des courbes présentées sous leur forme d'équations algébriques. De nombreuses courbes telles que les caténaires, les cycloïdes (courbes tracées par un point situé sur une roue qui tourne) et les spirales ne s'écrivent pas facilement à l'aide d'équations algébriques.

Une équation Ce que les mathématiciens recherchaient, c'était une définition générale pour une courbe quelconque, et pas seulement pour des exemples particuliers. Camille Jordan proposa une théorie des courbes construite sur la définition d'une courbe en termes de points variables.

En voici un exemple. Si l'on pose $x = t^2$ et $y = 2t$, alors, pour différentes valeurs de t on obtient de nombreux points différents dont on peut donner les coordonnées



Une courbe de Jordan simple et fermée

(x,y). Si par exemple $t = 0$, on obtient le point (0, 0), $t = 1$ donne le point (1, 2) et ainsi de suite. Si l'on trace ces points dans le repère (Ox), (Oy) et que l'on « relie les points entre eux », on obtient une parabole. Jordan affina cette idée de points reliés. Pour lui, c'était la définition d'une courbe.

Les courbes de Jordan peuvent être compliquées, même lorsqu'elles sont « simples » (elles ne se croisent pas) et « fermées » (elles n'ont ni début ni fin) comme le cercle. Le célèbre théorème de Jordan stipule qu'une courbe simple fermée a un intérieur et un extérieur. Son apparente « évidence » est un leurre.

En Italie, Giuseppe Peano fit sensation lorsqu'il montra en 1890 que, selon la définition de Jordan, un carré plein est une courbe. Il était possible d'arranger les points dans un carré de sorte qu'ils pouvaient tous être « reliés » selon la définition de Jordan. On appela ce type de courbe une courbe de Peano et on écorna au passage la définition de Jordan : il est clair qu'un carré n'est pas une courbe au sens conventionnel.

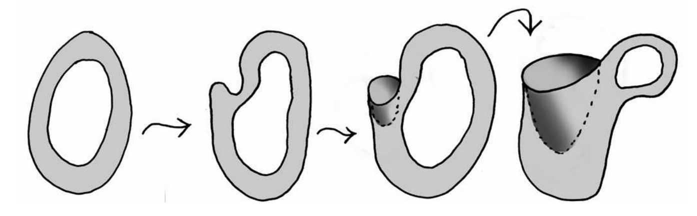
Les exemples de courbes de Peano et les autres exemples pathologiques obligèrent les mathématiciens à reprendre leur table à dessin et à réfléchir aux fondements de la théorie des courbes. Il s'agissait de développer une meilleure définition d'une courbe. Au début du XXe siècle, cette tâche conduisit les mathématiques dans ce nouveau domaine que constitue la topologie.

l'idée clé
Prendre le tournant

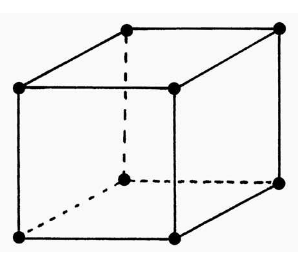
23 La topologie

La topologie est cette branche de la géométrie qui traite des propriétés des surfaces et des formes mais qui ne s'intéresse pas aux mesures de leurs longueurs ou de leurs angles. Sont primordiales en topologie les propriétés qui demeurent inchangées lorsque les formes se déforment. On peut étirer la forme étudiée dans tous les sens et c'est pourquoi la topologie est souvent décrite comme la « géométrie de la feuille de caoutchouc » ou géométrie des transformations continues. Les topologues sont des gens qui ne font pas la différence entre un donut et une tasse à café !

Un donut est une surface percée d'un trou en son milieu. Une tasse à café n'est pas différente, mais le trou prend la forme d'une anse. Voici comment on peut transformer un donut en tasse à café :



Classification des polyèdres Les formes les plus élémentaires étudiées par les topologues sont les polyèdres (« poly « signifiant « nombreux « et « èdre « signifiant « face »). Comme exemple de polyèdre, on peut citer le cube, qui a 6 faces carrées, 8 sommets (les points situés à la jonction des faces) et 12 côtés (les arêtes qui relient les sommets). Le cube est un polyèdre régulier parce que :



- toutes ses faces sont de forme identique et régulière,
- tous ses angles délimités par les arêtes qui se rencontrent aux différents sommets sont égaux.

La topologie est un domaine relativement neuf que l'on peut malgré tout faire remonter aux Grecs de l'Antiquité. Le plus

chronologie

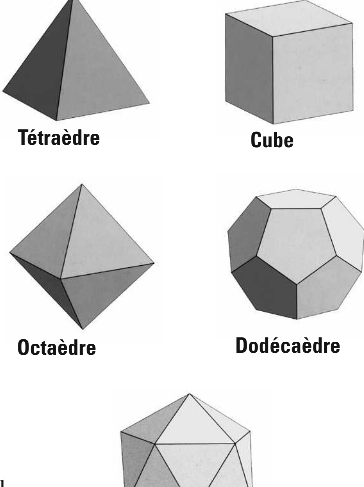
Vers 300 av. J.-C.
Euclide montre qu'il existe cinq polyèdres réguliers

250 ap. J.-C.
Archimède étudie les polyèdres tronqués.

1752
Euler donne sa formule pour trouver le nombre de sommets, arêtes et faces d'un polyèdre.

grand résultat présenté dans les *Éléments* d'Euclide montre qu'il y a exactement cinq polyèdres réguliers. Voici les solides de Platon :

- le tétraèdre (4 faces triangulaires)
- le cube (6 faces carrées)
- l'octaèdre (8 faces triangulaires)
- le dodécaèdre (12 faces pentagonales)
- l'icosaèdre (20 faces triangulaires).



Icosaèdre

Si l'on abandonne l'hypothèse selon laquelle toutes les faces sont identiques, nous nous retrouvons dans le monde des solides semi-réguliers d'Archimède. Des exemples peuvent être générés à partir des solides de Platon. Si l'on coupe (ou tronque) les coins de l'icosaèdre, on obtient la forme du ballon de foot actuel. Les 32 faces qui forment les pans sont constituées de 12 pentagones et de 20 hexagones. Il y a 90 côtés et 60 sommets. C'est aussi la forme des molécules buckminsterfullerènes, du nom du scientifique visionnaire Richard Buckminster Fuller, créateur du dôme géodésique. Ces « buckyballes » sont une forme de carbone récemment découverte, le C_{60}, dont chaque sommet correspond à un atome de carbone.

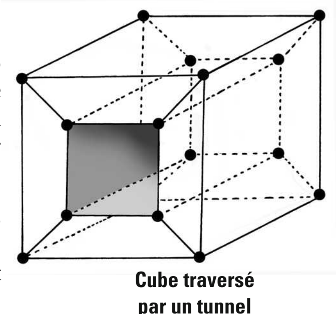
Icosaèdre tronqué

La formule d'Euler Selon la formule d'Euler, les nombres de sommets (S), d'arêtes (A) et de faces (F) d'un polyèdre sont liés par la formule

$$S - A + F = 2.$$

Pour un cube par exemple, S = 8, A = 12, et F = 6, et donc S – A + F = 8 – 12 + 6 = 2, et, pour les buckminsterfullerènes, S – A + F = 60 – 90 + 32 = 2. Ce théorème remet en fait en question la notion même de polyèdre.

Si un cube est traversé par un « tunnel », est-ce un vrai polyèdre ? Pour cette forme, S = 16, A = 32, F = 16 et S – A + F = 16 – 32 + 16 = 0. La formule d'Euler ne fonctionne pas. Pour que la formule soit à nouveau correcte, on pourrait se limiter aux polyèdres qui ne comportent pas de tunnel. Ou alors, on pourrait généraliser la formule pour inclure cette particularité.



Cube traversé par un tunnel

La classification des surfaces Un topologue peut très bien considérer que le donut et la tasse à café sont identiques, mais quel genre de surface est différent du donut ? On peut penser à la balle en caoutchouc. Il n'existe aucune façon de

1858
Möbius et Listing présentent le ruban de Möbius.

1961
Stephen Smale prouve la conjecture de Poincaré en dimension supérieure à 4.

1982
Michael Freedman prouve la conjecture de Poincaré en dimension égale à 4.

2002
Perelman prouve la conjecture de Poincaré pour la dimension 3.

transformer le donut en balle puisque le donut comporte un trou, à l'inverse de la balle. C'est ce qui différencie fondamentalement ces deux surfaces. On peut donc classer les surfaces en fonction du nombre de trous qu'elles contiennent.

Prenons une surface contenant *r* trous, et divisons-la en régions limitées par des arêtes joignant les sommets. Cela fait, on peut compter le nombre de sommets, d'arêtes et de faces. Pour toute division, la formule d'Euler S – A + F a une valeur constante, appelée la caractéristique d'Euler de la surface (ou d'Euler-Poincaré) :

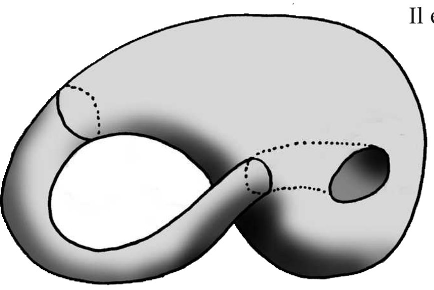
$$S - A + F = 2 - 2r.$$

Si la surface ne contient aucun trou ($r = 0$) comme c'était le cas pour le polyèdre ordinaire, la formule se réduit à la formule d'Euler S – A + F = 2. S'il y a un trou, ($r = 1$), comme dans l'exemple du cube percé d'un tunnel, S – A + F = 0.

Les surfaces à un seul côté Une surface comporte d'ordinaire deux faces. L'extérieur d'une balle est différent de son intérieur et la seule façon de passer d'un côté à l'autre est de percer un trou dans la balle, opération de découpage non autorisée en topologie (on peut étendre les surfaces mais pas les couper). Un morceau de papier est un autre exemple de surface à deux faces. Le seul endroit où un côté rencontre l'autre, c'est le long de la frontière formée par les deux côtés du papier.

Le ruban de Möbius

L'idée d'une surface à une seule face semble bizarre. Néanmoins, une telle surface, célèbre aujourd'hui, a été découverte par le mathématicien et astronome allemand August Möbius au XIXe siècle. Pour la construire, on prend une bande de papier, on lui fait subir une torsion et on colle les deux extrémités. Le résultat est un « ruban de Möbius », surface à une seule face et un bord courbe. Vous pouvez prendre votre crayon et commencer à tracer une droite en son milieu. Très vite, vous revenez à votre point de départ !



La bouteille de Klein

Il est même possible d'avoir une surface à une seule face et sans bord. C'est la « bouteille de Klein », qui doit son nom au mathématicien allemand Félix Klein. Ce qui est particulièrement impressionnant avec cette bouteille, c'est qu'elle ne se coupe pas elle-même. Cependant, il n'est pas possible de représenter une bouteille de Klein dans l'espace à trois dimensions sans avoir d'intersection physique, car l'espace qui lui convient est l'espace à quatre dimensions, qui autorise cette absence d'intersection.

Ces deux surfaces sont des exemples de ce que les topologues appellent des « variétés topologiques », c'est-à-

dire des surfaces géométriques qui ressemblent à des morceaux de papier à deux dimensions lorsque de petites portions sont vues par elles-mêmes. Étant donné que la bouteille de Klein n'a pas de bord, on dit que c'est une variété « fermée » de dimension 2.

La conjecture de Poincaré Pendant plus d'un siècle, le problème le plus important en topologie demeura la conjecture de Poincaré, du nom d'Henri Poincaré qui la formula. La conjecture se situe aux confluents de l'algèbre et de la topologie.

La partie de la conjecture non résolue jusqu'à ces dernières années concernait les variétés fermées de dimension 3. En effet, ces variétés peuvent être très compliquées : imaginez une bouteille de Klein de dimension supérieure. Poincaré conjectura que certaines variétés fermées de dimension 3 qui ont toutes les propriétés de sphères à trois dimensions sont en réalité nécessairement des sphères. Imaginez que vous faites le tour d'un ballon géant : vous ne recevrez que des indices qui indiquent qu'il s'agit d'une sphère, mais, comme vous ne pouvez pas la visualiser, vous ne saurez pas si c'est véritablement le cas.

Personne ne réussit à prouver la conjecture de Poincaré pour les variétés de dimension 3. Était-elle vraie ou fausse ? On avait réussi à en apporter la preuve pour d'autres dimensions mais le problème de la variété de dimension 3 était récalcitrant. Plusieurs preuves incorrectes furent produites, mais en 2002, Grigori Perelman, de l'institut de mathématiques de Steklov à Saint Petersbourg, annonça qu'il l'avait enfin prouvée. La preuve a finalement été validée le 22 août 2006. À l'instar des solutions d'autres grands problèmes, les techniques utilisées pour la résoudre se trouvaient en dehors du champ immédiat des mathématiques : il s'agissait d'une technique liée à la diffusion de la chaleur.

l'idée clé
Des donuts aux tasses à café

24 La dimension

Léonard de Vinci écrivit dans ses carnets : « La science de la peinture commence avec le point, puis vient la droite, le plan vient en troisième position suivi par le corps dans son drapé de plans. » Dans la hiérarchie de de Vinci, le plan est à deux dimensions et l'espace à trois dimensions. Que peut-il y avoir de plus clair ? C'est de cette manière que le point, la droite, les géométries dans le plan ou dans l'espace ont été présentés par le géomètre grec Euclide, et Léonard travaillait dans le même esprit.

On a pensé pendant des millénaires que l'espace physique avait trois dimensions. Dans l'espace physique, on peut quitter cette page en suivant l'axe des x, la traverser horizontalement en suivant l'axe des y ou verticalement en remontant l'axe des z, ou encore combiner tous ces déplacements. On localise un point par rapport à l'origine du repère (le point où se rencontrent les trois axes) qui lui donne ses coordonnées précisées par les valeurs de x, y, et z qui s'écrivent sous la forme (x, y, z).

Un cube, comme les autres solides, est évidemment à trois dimensions. Normalement à l'école, on apprend la géométrie plane qui est de dimension deux, ensuite on passe à la géométrie à trois dimensions, ou « géométrie dans l'espace », et on s'arrête là.

z
y
x

L'espace de dimension 3

Vers le début du XIX[e] siècle, les mathématiciens ont commencé, l'air de rien, à toucher à la dimension 4, et même à des mathématiques de dimensions supérieures. De nombreux philosophes et mathématiciens commencèrent à s'interroger sur l'existence de ces dimensions supérieures.

Des dimensions physiques supérieures De nombreux grands mathématiciens pensaient jadis qu'un espace à quatre dimensions était inconcevable. Ils restaient sceptiques quant à la réalité de ces quatre dimensions, et en apporter l'explication devint le nouveau défi à relever.

chronologie

Vers 300 av. J.-C.
Euclide décrit un monde à trois dimensions.

1877 ap. J.-C.
Cantor est surpris par l'ampleur des controverses que suscitent ses découvertes sur la théorie des dimensions.

D'ordinaire, pour expliquer pourquoi il est possible d'avoir quatre dimensions, on revient à l'espace à deux dimensions. En 1884, un maître d'école et théologien anglais, Edwin Abbott, rencontra un vif succès avec son livre *Flatland*, dont les personnages, appelés Flatlanders, habitent un monde à deux dimensions. Ces êtres ne voient pas les triangles, les carrés ni les cercles qui existent dans leur pays parce qu'ils n'ont pas accès à la troisième dimension. Leur vision est extrêmement limitée. Il leur est aussi difficile de se représenter une troisième dimension que pour nous d'imaginer la quatrième dimension. Toutefois, lire Abbott nous met dans une disposition d'esprit favorable pour accepter cette quatrième dimension.

Le besoin d'envisager l'existence d'un espace à quatre dimensions se fit plus urgent avec l'arrivée d'Einstein. La géométrie à quatre dimensions parut alors plus vraisemblable et même plus compréhensible parce que la dimension supplémentaire que le modèle d'Einstein introduisit est le temps. Contrairement à Newton, Einstein conçut le temps comme lié à l'espace dans un continuum espace-temps à quatre dimensions. Einstein décréta que nous vivons dans un monde à quatre dimensions doté de quatre coordonnées (x, y, z, t), où t désigne le temps.

Ce monde à quatre dimensions d'Einstein a tout d'un poncif aujourd'hui. Il existe un modèle plus récent de réalité physique qui repose sur des « cordes ». Dans cette théorie, les particules subatomiques familières telles que les électrons ne sont que les effets de la vibration légère à laquelle sont soumises de minuscules cordelettes. La théorie des cordes implique le remplacement du continuum espace-temps à quatre dimensions par une version qui en comporte davantage. Selon la recherche actuelle, pour tenir compte de la théorie des cordes, la dimension du continuum espace-temps devrait être élargie à 10, 11 ou 26 dimensions en fonction des hypothèses et des différents points de vue adoptés.

Un énorme aimant de 2 000 tonnes utilisé au CERN de Genève, en Suisse, et conçu pour provoquer des collisions de particules à vitesses élevées, pourrait aider à résoudre le problème. Créé pour découvrir la structure de la matière, il pourrait, en prime, permettre d'accéder à une meilleure théorie et apporter une réponse « correcte » au problème des dimensions. La conclusion, c'est que nous vivons peut-être dans un univers à 11 dimensions.

L'hyper-espace Contrairement à ce qui se passe en physique avec les dimensions supérieures, il n'y a absolument aucun problème à imaginer un espace mathématique à plus de trois dimensions.

On peut représenter l'espace mathématique avec autant de dimensions que l'on veut. Depuis le début du XIX[e] siècle, les mathématiciens utilisent en général dans leurs calculs des variables notées n. George Green, meunier de Nottingham qui explorait les mathématiques de l'électricité, et de purs mathématiciens tels que

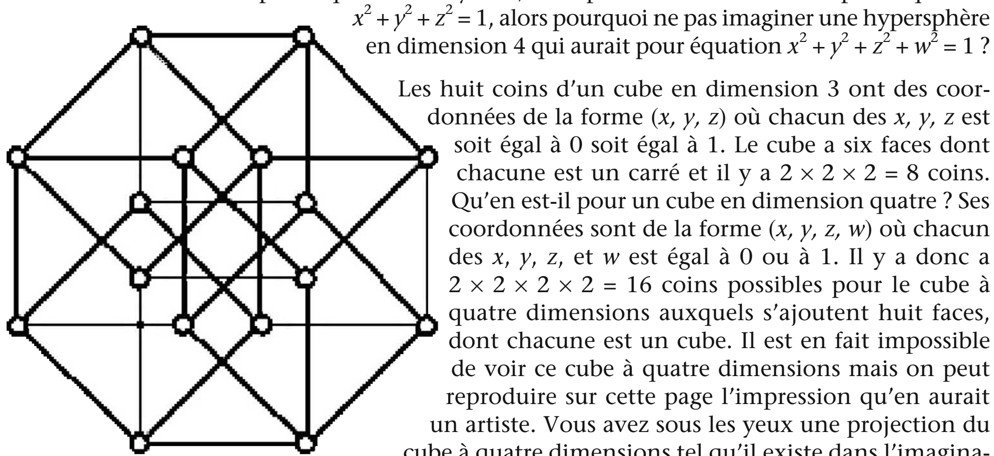
1909
Les travaux de Brouwer modifient la notion que nous avons de la dimension.

1919
Hausdorff introduit la notion de « dimension d'Hausdorff » ou dimension fractale.

1970
La théorie des cordes voit notre univers comme un espace à 10, 11, ou 26 dimensions.

Augustin-Louis Cauchy, Arthur Cayley et Hermann Grassmann, ont tous décrit les mathématiques en termes d'un espace de dimension n. Il n'y avait, semble-t-il, aucune raison de limiter les mathématiques et ce faisant, de se priver de tout ce que l'on pouvait gagner en élégance et en clarté.

L'idée des n dimensions n'est qu'une extension des coordonnées (x, y, z) de la dimension 3 à un nombre non spécifié de variables. Un cercle en dimension 2 a pour équation $x^2 + y^2 = 1$, une sphère en dimension 3 a pour équation $x^2 + y^2 + z^2 = 1$, alors pourquoi ne pas imaginer une hypersphère en dimension 4 qui aurait pour équation $x^2 + y^2 + z^2 + w^2 = 1$?



Le cube à quatre dimensions

Les huit coins d'un cube en dimension 3 ont des coordonnées de la forme (x, y, z) où chacun des x, y, z est soit égal à 0 soit égal à 1. Le cube a six faces dont chacune est un carré et il y a $2 \times 2 \times 2 = 8$ coins. Qu'en est-il pour un cube en dimension quatre ? Ses coordonnées sont de la forme (x, y, z, w) où chacun des x, y, z, et w est égal à 0 ou à 1. Il y a donc a $2 \times 2 \times 2 \times 2 = 16$ coins possibles pour le cube à quatre dimensions auxquels s'ajoutent huit faces, dont chacune est un cube. Il est en fait impossible de voir ce cube à quatre dimensions mais on peut reproduire sur cette page l'impression qu'en aurait un artiste. Vous avez sous les yeux une projection du cube à quatre dimensions tel qu'il existe dans l'imagination du mathématicien. On parvient ainsi à entrevoir les faces de ce cube.

L'espace à plusieurs dimensions est familier aux spécialistes des mathématiques pures. Personne ne prétend qu'un tel espace existe réellement même si l'on peut supposer qu'il existe dans un monde Platonique idéal. Dans le grand problème de la classification des groupes par exemple, « le groupe des monstres » (voir page 155) permet de mesurer la symétrie dans un espace mathématique à 196 883 dimensions. On ne peut pas « voir » cet espace comme on le fait dans l'espace ordinaire à trois dimensions, mais on peut quand même l'imaginer et l'utiliser d'une manière précise grâce à l'algèbre moderne.

L'intérêt que les mathématiciens portent aux dimensions n'a absolument rien à voir avec ce qu'est l'analyse dimensionnelle pour le physicien. Les unités de grandeur de la physique se mesurent en termes de masse M, longueur L, et temps T. En analyse dimensionnelle, un physicien peut donc vérifier que les équations sont justes en en comparant les deux membres, qui doivent avoir la même dimension.

On ne peut pas avoir l'égalité force = vitesse. Une analyse dimensionnelle donne la vitesse en mètres par seconde. La dimension d'une vitesse est donc une longueur divisée par un temps, soit L/T, que l'on écrit LT^{-1}. La force a la dimension d'une

masse multipliée par l'accélération, et puisque l'accélération est égale à des mètres par seconde au carré, la force aura donc pour dimension MLT^{-2}.

La topologie La théorie des dimensions est une partie de la topologie générale. D'autres concepts de la dimension peuvent être définis indépendamment en termes d'espaces mathématiques abstraits. Une tâche majeure est de montrer comment ils sont reliés entre eux. De grands mathématiciens, spécialisés dans des domaines différents, ont approfondi la signification de la dimension, comme par exemple Henri Lebesgue, L.E.J. Brouwer, Karl Menger, Paul Urysohn et Leopold Vietoris (qui fut le doyen de l'Autriche et qui est décédé en 2002 à l'âge de 110 ans).

L'ouvrage clé sur le sujet s'intitule *Dimension Theory*. Publié en 1948 par Witold Hurewicz et Henry Wallman, il a, pense-t-on encore aujourd'hui, révolutionné notre compréhension du concept de dimension.

La dimension sous toutes ses formes Les trois dimensions introduites par les Grecs ont permis l'analyse critique du concept de dimension, puis son extension.

Personnes coordonnées

Les êtres humains sont eux-mêmes des objets à plusieurs dimensions. Un être humain a plus de trois « coordonnées ». On pourrait utiliser (*a, b, c, d, e, f, g, h*) pour représenter l'âge, la taille, le poids, le genre, la pointure, la couleur des yeux, celle des cheveux, la nationalité, et ainsi de suite. On pourrait alors remplacer les points géométriques par des personnes. En nous limitant à cet « espace » à huit dimensions, John Doe aurait pour coordonnées (43 ans, 1 m 65, 83 kg, masculin, 42, bleus, blonds, danois) et pour Marie Martin, ce serait (26 ans, 1 m 57, 56 kg, féminin, 37, noisette, châtains, française).

Les *n* dimensions de l'espace mathématique ont pu être introduites sans trop de difficulté. Quant aux physiciens, ils ont fait reposer leurs théories sur la notion d'espace-temps (de dimension 4) et sur des versions récentes de la théorie des cordes (voir page 97) qui exigent 10, 11 et 26 dimensions. On fit quelques incursions dans les dimensions fractionnelles avec les formes fractales (voir page 100), incursions qui se sont accompagnées d'une étude de différentes mesures. Hilbert introduisit un espace de dimension infinie devenu aujourd'hui un cadre essentiel pour les mathématiques pures. La dimension dépasse largement la géométrie euclidienne à une, deux, et trois dimensions.

l'idée clé
Au-delà de la troisième dimension

25 Les fractales

En mars 1980, l'unité centrale ultramoderne du centre de recherche IBM à Yorktown Heights, dans l'État de New York, donnait ses instructions à un vieux système d'impression Tektronix. Des points étaient consciencieusement disséminés en des endroits curieux d'une page blanche, et au final, on aurait dit que l'on s'était amusé à éparpiller une poignée de grains de poussières sur la page. Benoît Mandelbrot se frotta les yeux, incrédule. Il comprit qu'il assistait à quelque chose d'important, sans savoir quoi. L'image se formait lentement devant lui comme une photo en noir et blanc qu'un révélateur fait apparaître peu à peu. C'était un premier aperçu de cette icône dans le monde des fractals que l'on appelle l'ensemble de Mandelbrot.

Voilà un exemple type de ces mathématiques expérimentales qui permettent d'aborder les problèmes de manière empirique comme le font les physiciens et les chimistes dans leur laboratoire. Les mathématiciens aussi pouvaient maintenant mener des expériences. De nouvelles perspectives, au sens propre du terme, s'ouvraient à eux. Ils pouvaient ainsi échapper à ce carcan de « définitions, théorèmes, et preuves », même si un retour aux rigueurs d'un raisonnement logique était inévitable. Ce serait toutefois pour plus tard.

L'approche expérimentale présentait l'inconvénient de partir d'images visuelles pour aboutir à l'étayage d'une théorie. Les expérimentateurs naviguaient à vue. Ainsi, Mandelbrot forgea le mot « fractal » sans savoir de quoi il s'agissait. Une définition précise pouvait-elle être donnée comme cela se fait d'ordinaire en mathématiques ? Au départ, Mandelbrot s'y refusa. Il ne voulait pas détruire la magie de l'expérience avec une définition soigneusement élaborée mais peut-être inappropriée et contraignante. Il sentit que le concept de fractal était « comme un bon vin : il lui fallait vieillir un peu avant la mise en bouteille ».

L'ensemble de Mandelbrot La démarche de Mandelbrot et de ses collègues mathématiciens n'avait rien de particulièrement abscons. Ils manipulaient les formules les plus simples qui soient. Tout repose sur l'idée d'itération puisqu'il s'agit d'appliquer une formule de manière répétée. Celle qui est à l'origine de l'ensemble de Mandelbrot s'écrivait simplement comme suit : $x^2 + c$

chronologie

1879
Cayley étudie un précurseur des ensembles fractals modernes.

1904
von Koch crée sa courbe en flocon de neige.

Pour commencer, il faut choisir une valeur de c. Prenons $c = 0{,}5$. Si l'on commence avec $x = 0$, le premier calcul donne encore 0,5. On prend maintenant $x = 0{,}5$ et le deuxième calcul s'écrit donc : $(0{,}5)^2 + 0{,}5 = 0{,}75$. On continue, et le troisième calcul donne $(0{,}75)^2 + 0{,}5 = 1{,}0625$. Tous ces calculs peuvent s'effectuer sur une simple calculatrice. Si l'on poursuit ainsi, on observe que le résultat obtenu est en constante augmentation.

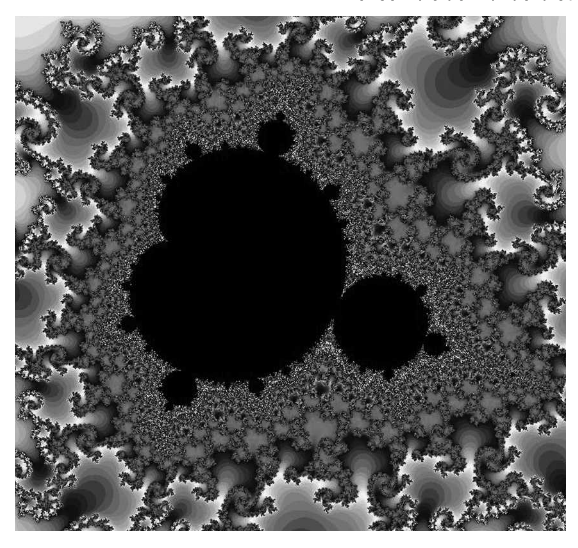
Essayons avec une autre valeur de c. Cette fois, $c = -\,0{,}5$. Comme précédemment, on commence avec $x = 0$. La formule $x^2 - 0{,}5$ a pour résultat – 0,5. Si l'on poursuit, on obtient – 0,25, mais cette fois, les valeurs n'augmentent plus. Après quelques oscillations, elles se stabilisent vers une valeur proche de – 0,3660…

En prenant $c = 0{,}5$, la suite qui commence à $x = 0$ monte en chandelle avant de tendre vers l'infini, mais avec $c = -\,0{,}5$, on observe que la suite qui commence à $x = 0$ tend vers une valeur proche de – 0,3660. L'ensemble de Mandelbrot est constitué de toutes ces valeurs de c pour lesquelles la suite commençant à $x = 0$ ne tend pas vers l'infini.

L'histoire ne s'arrête pas là. Nous ne nous sommes occupé jusqu'à présent que des nombres réels (nombres de dimension 1). Le résultat obtenu est un ensemble de Mandelbrot de dimension 1 qui ne montre pas grand-chose. Il faut prendre la même formule $z^2 + c$ mais cette fois z et c sont deux nombres complexes (nombres de dimension 2 – voir page 32). On obtient alors un ensemble de Mandelbrot de dimension 2.



L'ensemble de Mandelbrot



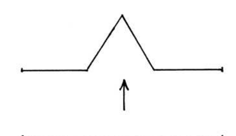
Pour certaines valeurs de c prises dans l'ensemble de Mandelbrot, la suite de z peut accomplir toutes sortes de choses bizarres comme évoluer entre plusieurs points mais ne pas s'échapper vers l'infini. Dans cet ensemble, une autre propriété clé des ensembles fractals apparaît : celle de similitude. Si vous zoomez sur l'intérieur de l'ensemble, vous ne serez pas sûr de l'échelle parce que vous ne verrez rien de plus que d'autres ensembles de Mandelbrot.

Avant Mandelbrot Comme souvent en mathématiques, les découvertes sont rarement toutes neuves. L'histoire apprit à Mandelbrot que l'idée avait déjà effleuré l'esprit de mathématiciens tels qu'Henri Poincaré et Arthur Cayley cent ans auparavant. Malheureusement, ils

1918
Hausdorff introduit le concept de dimension fractale.

1919
Julia et Fatou étudient les structures fractales dans le plan complexe.

1975
Mandelbrot introduit le terme « fractal ».



L'élément générateur du flocon de von Koch

ne disposaient pas de la puissance informatique nécessaire pour pousser plus avant leurs recherches.

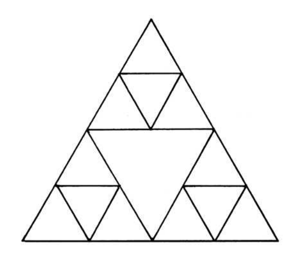
Les formes découvertes par la première vague des théoriciens des courbes fractales incluaient des courbes crêpelées et les « courbes monstres » auparavant qualifiées de cas pathologiques et rejetées à ce titre. Parce qu'elles étaient pathologiques, on les avait enfermées dans le placard du mathématicien et on n'y avait prêté que peu attention. On voulait alors ces courbes « régulières » et plus ordinaires que l'on pouvait traiter avec le calcul différentiel. La popularité des ensembles fractals permit d'exhumer le travail d'autres mathématiciens tels que Gaston Julia et Pierre Fatou qui travaillèrent sur des structures similaires dans le plan complexe juste après la Première Guerre Mondiale. Leurs courbes n'étaient alors pas qualifiées de fractales, bien sûr, et ils ne disposaient pas de tout l'équipement technologique nécessaire pour voir leurs formes.

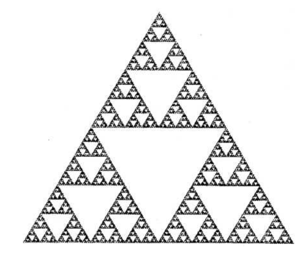
D'autres courbes fractales célèbres La célèbre courbe de von Koch tient son nom du mathématicien suisse Niels Helge von Koch. La courbe du flocon est l'une des premières courbes fractales. On peut la créer à partir du côté d'un triangle équilatéral que l'on coupe en trois segments de même longueur. On utilise le segment central pour servir de base à un autre triangle équilatéral.

La courbe de von Koch présente une particularité curieuse : c'est une aire finie, parce qu'elle reste à l'intérieur d'un cercle, mais à chaque itération, sa longueur s'accroît. C'est une courbe qui contient une aire finie mais dont le périmètre est « infini » !

Le flocon de von Koch

Une autre courbe fractale célèbre tient son nom du mathématicien polonais Waclaw Sierpiński. Pour la générer, on retire des triangles équilatéraux d'un triangle équilatéral ; si l'on poursuit ce processus, on obtient le triangle de Sierpiński (que l'on peut générer selon un processus différent – voir page 54).





Le triangle de Sierpiński

La dimension fractale Felix Hausdorff considéra la dimension d'une manière toute nouvelle. Il fit intervenir la notion d'échelle. Si une droite est augmentée proportionnellement par un facteur 3, elle est trois fois plus grande qu'au départ. Puisque $3 = 3^1$, on dit qu'une droite est de dimension 1. Si un carré est augmenté proportionnellement par un facteur 3, son aire est égale à 9 fois son aire initiale, soit 3^2, et la dimension est donc de dimension 2. Si un cube est augmenté proportionnellement par ce facteur, son volume est égal à 27 ou 3^3 et il est donc de dimension 3. Ces valeurs de la dimension de Hausdorff coïncident avec ce que nous attendons pour une droite, un carré, ou un cube.

Si l'unité de base de la courbe de von Koch est augmentée proportionnellement par 3, elle devient 4 fois plus grande que précédemment. En suivant le procédé décrit, la dimension de Hausdorff est égale à la valeur de D pour laquelle $4 = 3^D$. On peut aussi avoir cet autre calcul :

$$D = \frac{\ln 4}{\ln 3}$$

ce qui signifie que la dimension D, pour la courbe de von Koch, est à peu près égale à 1,262. Avec les courbes fractales, il arrive fréquemment que la dimension de Hausdorff soit plus grande que la dimension ordinaire, qui est égale à 1 dans le cas de la courbe de von Koch.

La dimension de Hausdorff entre dans la définition que Mandelbrot donne d'un ensemble fractal qu'il présente comme un ensemble de points dont la valeur de D n'est pas un nombre entier. La dimension fractale devint la propriété clé des ensembles fractals.

Les applications des ensembles fractals Les ensembles fractals ont un vaste champ d'applications potentielles. Ils pourraient très bien être le principe mathématique qui entre dans la modélisation de phénomènes naturels tels que la croissance des plantes ou la formation des nuages.

Les ensembles fractals trouvent déjà des applications dans la croissance d'organismes marins comme les coraux et les éponges. On a démontré que l'extension des villes modernes présente des similitudes avec la croissance fractale. En médecine, ils sont utilisés dans la modélisation de l'activité cérébrale. La nature fractale des mouvements financiers en bourse ou sur les marchés de change a aussi été explorée. Les travaux de Mandelbrot inaugurèrent un nouveau point de vue, et il reste encore beaucoup à découvrir.

l'idée clé
Les formes de dimension fractale

26 Le chaos

Comment une théorie du chaos est-elle possible ? Le chaos ne se produit-il justement pas en l'absence de toute théorie ? L'histoire remonte à 1812. Alors que Napoléon avançait sur Moscou, son compatriote le Marquis Pierre-Simon de Laplace publia un essai sur le déterminisme universel : si, à un moment particulier, on connaissait la position et la vitesse de tous les objets de l'Univers, ainsi que les forces qui agissent sur eux, on pourrait alors calculer ces quantités de manière exacte pour tous les moments à venir. L'Univers et tous les objets qui s'y trouvent seraient complètement déterminés. La théorie du chaos nous montre que le monde est bien plus compliqué que cela.

Dans le monde réel, on ne peut pas connaître avec une précision absolue toutes les positions, vitesses et forces qui s'exercent, mais cette idée émise par Laplace avait pour corollaire que, si l'on disposait de valeurs approximatives à un instant donné, on ne serait pas loin d'avoir une image exacte de l'Univers. C'était raisonnable, car les sprinters qui démarrent un dixième de seconde après le signal de départ franchissent la ligne d'arrivée seulement un dixième de seconde après leur temps habituel. On pensait que de petits écarts dans les conditions initiales signifiaient de petits écarts dans le résultat. La théorie du chaos vint détruire cette idée.

L'effet papillon L'effet papillon montre comment une modification infime des conditions initiales peut produire un résultat très différent de celui que l'on attend. Si l'on prévoit du beau temps en Europe, mais si un papillon bat des ailes en Amérique du Sud, on peut craindre des tempêtes de l'autre côté de la planète, parce que le battement d'ailes modifie très légèrement la pression de l'air, provoquant ainsi un schéma météorologique complètement différent de celui qui était initialement prévu.

On peut illustrer cette idée à l'aide d'une expérience simple. Si vous laissez tomber une bille par l'ouverture d'une planche à clous (ou planche de Galton), la bille descendra et sera déviée dans sa chute d'un côté ou de l'autre en fonction des différents clous qu'elle rencontrera sur sa trajectoire avant d'atteindre l'une des colonnes d'arrivée. Vous pouvez essayer de faire tomber une bille identique à partir de la même position et avec une vitesse absolument identique. Si vous réussissez à procéder exactement de la même façon, alors le Marquis de Laplace aurait raison et la trajectoire suivie par la balle serait exactement la même. Si la première bille

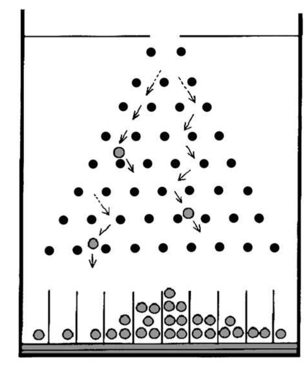
chronologie

1812
Laplace publie son essai sur le déterminisme universel.

1889
Poincaré développe le concept de chaos alors qu'il travaille sur le problème des trois corps pour lequel il fut récompensé par le grand Prix de Suède décerné par le Roi Oscar.

tombait dans la troisième colonne à partir de la droite, alors il en irait de même pour la deuxième.

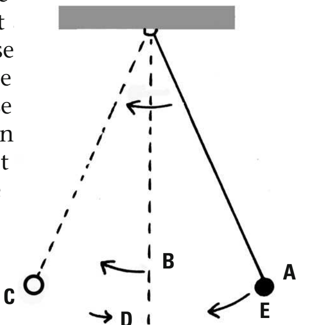
Mais bien sûr, il est impossible de faire tomber la bille à partir de la même position, avec la même vitesse et la même force. En réalité, il y a toujours une toute petite différence que l'on n'est peut-être même pas capable de mesurer. Au final, il est possible que la bille suive une trajectoire très différente et termine sa course dans une colonne différente.


La planche de Galton

Un pendule simple Le pendule libre est l'un des systèmes mécaniques d'analyse les plus simples qui soient. À mesure que le pendule se balance d'avant en arrière, il perd peu à peu de l'énergie. La masse s'écarte de moins en moins de la verticale et perd de sa vitesse (angulaire), avant de s'immobiliser complètement.

Le mouvement de la masse peut être représenté sous la forme d'un diagramme de phase. On mesure le déplacement (angulaire) sur l'axe des abscisses, et la vitesse sur l'axe des ordonnées. Le point d'où la masse est lâchée est représenté par le point A placé sur l'axe des abscisses. Au point A, le déplacement est à son maximum et la vitesse est nulle. Lorsque la masse passe par l'axe des ordonnées (à l'endroit où le déplacement est nul), la vitesse est son maximum, ce qui est représenté sur le diagramme de phase par le point B. La masse atteint l'autre extrémité de sa trajectoire au point C où le déplacement est négatif et la vitesse nulle. Le poids revient alors en passant par D (il se déplace dans la direction inverse et sa vitesse est donc négative) et achève un mouvement de va-et-vient complet en E. Le diagramme de phase représente ce mouvement par une rotation de 360°, mais le point E est représenté à l'intérieur du point origine A parce que le mouvement s'est affaibli. Comme le balancement du pendule diminue, le portrait de phase revient à l'origine du repère en effectuant une spirale jusqu'à l'immobilisation complète du pendule.

Un pendule simple



Ce n'est pas la même chose avec le pendule double dont la masse est à l'extrémité de deux tiges mises bout à bout. Si le déplacement est faible, le mouvement du pendule double est semblable à celui du pendule simple, mais si le déplacement est ample, la masse exécute un mouvement de va-et-vient, pivote, puis fait des embardées, et le déplacement autour de l'articulation intermédiaire est alors apparemment aléatoire. Si le mouvement n'est pas contraint, la masse s'arrête aussi mais la courbe qui décrit son mouvement est très différente de la spirale bien nette du pendule simple.

1961
Lorenz observe l'effet papillon.

1971
Robert May étudie le chaos sur un modèle de population.

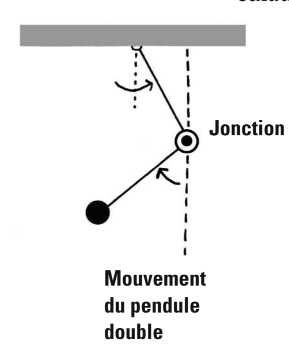
2004
La théorie du chaos passe dans la culture populaire avec le film *L'effet papillon*.

Vitesse
B
Déplacement
C D E A

Diagramme de phase du pendule simple

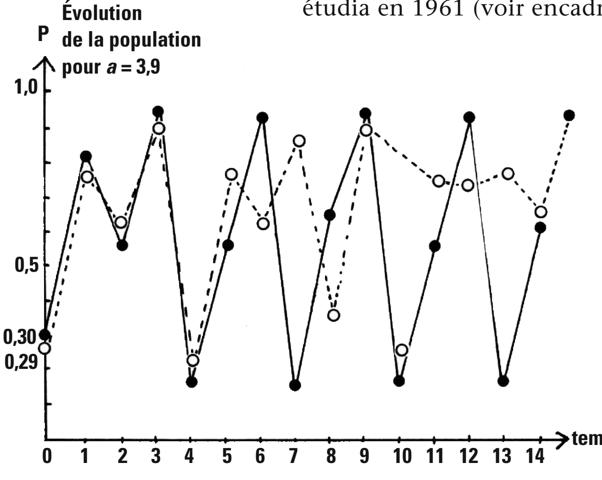
Le mouvement chaotique La caractéristique du chaos est qu'un système déterministe peut sembler générer un comportement aléatoire. Examinons un autre exemple, la formule répétitive ou itérative $a \times p \times (1 - p)$ où p représente la population, mesurée comme une probabilité sur une échelle allant de 0 à 1. La valeur de a doit être située quelque part entre 0 et 4 pour s'assurer que la valeur de p reste comprise entre 0 et 1.

Modélisons la population lorsque $a = 2$. Prenons par exemple $p = 0{,}3$ au temps $t = 0$. Pour trouver la population au temps $t = 1$, on remplace alors p par la valeur 0,3 dans la formule $a \times p \times (1 - p)$, ce qui donne 0,42. On peut répéter cette opération à l'aide d'une simple calculatrice uniquement, mais cette fois avec $p = 0{,}42$, ce qui nous donne le nombre suivant (0,4872). En progressant de cette manière, on trouve la population à des périodes plus avancées. Dans ce cas, la population se stabilise rapidement à $p = 0{,}5$. C'est toujours le cas pour des valeurs de a inférieures à 3.



Mouvement du pendule double

Si l'on choisit maintenant $a = 3{,}9$, valeur la plus proche possible du maximum autorisé, et si l'on utilise une population initiale identique $p = 0{,}3$, la population ne se stabilise pas mais oscille fortement. Cela est dû au fait que la valeur de a se trouve dans la « région chaotique », à savoir au-dessus de 3,57. De plus, si l'on choisit une population initiale différente $p = 0{,}29$, valeur proche de 0,3, la croissance de la population suit le schéma de la croissance précédente au début, mais s'en écarte ensuite complètement. C'est ce comportement qu'Edward Lorenz étudia en 1961 (voir encadré).



Évolution de la population pour $a = 3{,}9$

Les prévisions météorologiques Chacun sait que des ordinateurs, aussi puissants soient-ils, ne permettent pas de prévoir la météo plus de quelques jours à l'avance. Et même sur une période de quelques jours seulement, nous pouvons avoir de mauvaises surprises. Cela est dû au fait que les équations qui gouvernent le temps ne sont pas linéaires : elles mettent en jeu des variables multipliées entre elles, et d'autres choses encore.

La théorie mathématique qui gouverne les prévisions météorologiques fut élaborée par l'ingénieur français Claude Navier en 1821 ainsi que par le physicien mathématicien britannique George Gabriel Stokes en 1845. Les équations Navier-Stokes qui en résultèrent sont d'un très grand intérêt pour les scientifiques. L'Institut Mathématique Clay à Cambridge, dans le Massachusetts, a offert un prix d'un million de dollars à celui qui permettra des progrès considérables dans l'élaboration d'une théorie mathématique capable d'en révéler tous les secrets. Utilisées pour résoudre le problème de l'écoulement des fluides, elles nous apprennent beaucoup sur les mouvements réguliers de la haute atmosphère. Mais l'écoulement de l'air près de la surface de la Terre crée des turbulences responsables du chaos, avec les conséquences largement méconnues qu'il entraîne.

Alors que la théorie des systèmes linéaires d'équations est bien connue, les équations de Navier-Stokes contiennent des termes non linéaires qui les rendent difficiles à manipuler. Dans la pratique, la seule façon de les résoudre est de procéder numériquement en utilisant de puissants ordinateurs.

De la météorologie aux mathématiques

L'effet papillon fut découvert par hasard aux alentours de 1961. Lorsque le météorologiste Edward Lorenz, scientifique au MIT, partit prendre un café et laissa tourner son ordinateur, il fut très surpris par ce qu'il trouva à son retour. Il cherchait à saisir quelques modèles climatiques intéressants mais le nouveau graphique affiché sur son écran était méconnaissable. C'était étrange car il avait saisi dans l'ordinateur les mêmes valeurs initiales qui auraient donc dû produire la même image. Était-il temps de se débarrasser de ce vieil ordinateur pour un autre, plus fiable ?

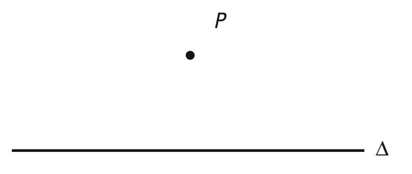
Après réflexion, il se rendit compte qu'il n'avait pas saisi les valeurs initiales de la même façon : la première fois, il s'était servi de six décimales mais ensuite, il n'en avait pris que trois. Pour expliquer cet écart entre les deux images obtenues, il inventa l'expression « effet papillon ». Après cette découverte, sa curiosité se tourna vers les mathématiques.

Des attracteurs étranges On peut considérer les systèmes dynamiques comme des systèmes qui possèdent des « attracteurs » dans leur diagramme de phase. Dans le cas du pendule simple, l'attracteur est le point d'origine, point unique vers lequel converge le mouvement. Avec le pendule double, c'est plus compliqué, mais même ici, le portrait de phase montre quelques régularités et sera attiré par un ensemble de points du diagramme de phase. Pour des systèmes comme celui-ci, l'ensemble de ces points forment un ensemble fractal (voir page 100), appelé un attracteur « étrange », dont la structure mathématique est définie. Alors, tout n'est pas perdu. Dans la nouvelle théorie du chaos, ce n'est pas tant un chaos chaotique qui en résulte qu'un chaos « ordonné ».

l'idée clé
Une régularité désordonnée

27 Le postulat des parallèles

Cette histoire tragique commence avec un scénario simple de géométrie. Imaginez une droite Δ et un point *p* n'appartenant pas la droite. Combien de droites pouvons-nous tracer qui passent par *p* et parallèles à la droite Δ ? Il semble évident qu'une droite et une seule passe par *p* sans jamais rencontrer Δ quelle que soit la distance sur laquelle on la prolongera dans un sens ou dans l'autre. Cela semble aller de soi et parfaitement respecter le bon sens. Euclide d'Alexandrie inclut une variante de cette règle au nombre des postulats qu'il énonce dans les *Éléments*, ouvrage fondamental de géométrie.



On ne peut pas toujours se fier au bon sens. Nous verrons si la supposition d'Euclide est cohérente d'un point de vue mathématique.

Les *Éléments* d'Euclide La géométrie d'Euclide est exposée dans les 13 livres des *Éléments*, ouvrage rédigé aux alentours de 300 av. J.-C. C'est l'un des textes les plus déterminants jamais écrits. Les mathématiciens grecs, qui voyaient en lui la première codification systématique de la géométrie, y faisaient d'ailleurs de constantes références. Plus tard, on l'étudia à l'université puis on le traduisit à partir des manuscrits conservés. Il fut ensuite transmis à la postérité et universellement présenté comme le modèle même de ce que devait être la géométrie.

On adapta les *Éléments* pour le rendre accessible aux écoliers et on se servit d'extraits du « livre sacré » pour enseigner la géométrie. On trouva cependant qu'il n'était pas adapté aux plus jeunes. Comme le poète A. C. Hilton le disait avec esprit : *« Though they wrote it all by rote, they did not write it right »* [« Ils la récitaient par cœur mais ils la connaissaient mal »]. On pourrait dire qu'Euclide écrivait pour les grands, et non pas pour les enfants. Dans les écoles anglaises, son influence atteignit son apogée dans le programme scolaire du XIXe siècle, mais il sert toujours de référence aux mathématiciens d'aujourd'hui.

chronologie

Vers 300 av. J.-C.
Euclide inclut le postulat du parallèle (le cinquième postulat) dans les *Éléments*.

1829–31 ap. J.-C.
Lobachevsky et Bolyai publient leur travail sur la géométrie hyperbolique.

Le style des *Éléments* d'Euclide en fait un ouvrage absolument remarquable : il accomplit la prouesse de présenter la géométrie comme une suite de propositions démontrées. Sherlock Holmes aurait admiré ce système de déduction qui progresse logiquement à partir de postulats clairement formulés. Il aurait pu fustiger le Dr Watson pour son incapacité à y voir un « système froid et dépourvu de passion ».

Les postulats d'Euclide

L'une des caractéristiques des mathématiques est que quelques suppositions peuvent générer de vastes théories. Les postulats d'Euclide en sont un excellent exemple car ils permirent de construire le modèle des systèmes axiomatiques futurs. Ses cinq postulats s'énoncent ainsi :

1. On peut tracer une droite et une seule qui passe par deux points quelconques.
2. Tout segment peut être prolongé en une droite.
3. On peut construire un cercle de centre quelconque et de rayon quelconque.
4. Tous les angles droits sont égaux entre eux.
5. Si une droite coupe deux droites et que la somme des angles intérieurs ainsi formés d'un côté est inférieure à deux angles droits, alors ces deux droites prolongées à l'infini sont sécantes en un point situé de ce côté où les angles sont inférieurs à deux angles droits.

Alors que tout l'édifice de la géométrie d'Euclide repose sur les postulats (que l'on appelle aujourd'hui des axiomes – voir encadré), ils n'étaient pas suffisants, et Euclide leur ajouta des « définitions » et des « notions communes ». Les définitions incluent des affirmations telles que : « Le *point* est ce dont la partie est nulle » et « Une *ligne* est une longueur sans épaisseur ». Les notions communes incluent des observations telles que « Le tout est plus grand que la partie » et « Des choses qui sont égales à une même chose sont égales entre elles ». Ce n'est que vers la fin du XIXe siècle que l'on reconnut qu'Euclide s'était livré à des suppositions tacites.

Le cinquième postulat Le cinquième postulat fut à l'origine d'une controverse plus de 2 000 ans après la première apparition des *Éléments*. De par son style d'abord, verbeux et lourd, il ne semble pas être à sa place. Euclide lui-même n'en était pas satisfait mais il ne pouvait en faire l'économie pour prouver certaines propositions. Il essaya en vain de le prouver à partir des autres postulats.

Le cinquième postulat d'Euclide

Plus tard, des mathématiciens ont essayé de le prouver ou encore de le remplacer par un postulat plus simple. En 1795, c'est la reformulation de John Playfair qui s'imposa : par un point P n'appartenant pas à une droite Δ, il n'existe qu'une seule droite

1854 Riemann donne des conférences sur les fondations de la géométrie.

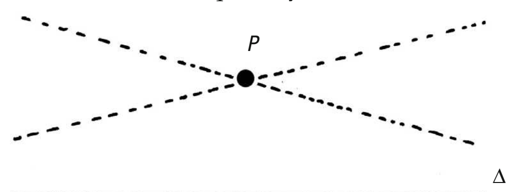
1872 Klein unifie la géométrie via la théorie des groupes.

1915 Einstein fait reposer sa théorie de la relativité sur la géométrie Riemannienne.

passant par *P* et parallèle à Δ. À peu près à la même époque, Adrien Marie Legendre lui substitua une autre version lorsqu'il affirma l'existence d'un triangle dont les angles ont pour somme 180°. Ces reformulations du cinquième postulat aidèrent à réfuter l'objection selon laquelle ce postulat était artificiel. Elles étaient plus acceptables que la version indigeste d'Euclide.

On a aussi cherché à trouver la preuve insaisissable du cinquième postulat. Cette recherche séduisait fortement ses adeptes. Si l'on avait pu trouver une preuve, le postulat serait devenu un théorème et c'en aurait été fait des critiques. Malheureusement, les tentatives furent toutes d'excellents exemples de raisonnement circulaire, raisonnement dont les arguments supposent la chose même qu'ils essaient de prouver.

La géométrie non euclidienne Une découverte capitale fut réalisée grâce au travail de Carl Friedrich Gauss, János Bolyai et Nikolai Ivanovich Lobachevsky. Gauss ne publia pas son travail, mais il semble évident qu'il parvint à ses conclusions en 1817. Bolyai publia le sien en 1831 et Lobachevsky, de son côté, en 1829, ce qui les entraîna dans une querelle de priorité. On ne peut douter du génie de ces hommes. Ils ont effectivement montré que le cinquième postulat était indépendant des quatre autres. En ajoutant sa négation aux quatre autres postulats, ils ont montré qu'un système cohérent était possible.



Bolyai et Lobachevsky construisirent une nouvelle géométrie en autorisant qu'il y ait plus d'une droite qui passe par *P* sans jamais rencontrer la droite Δ. Comment est-ce possible ? Il est certain que les droites en pointillés rencontrent Δ. Si l'on accepte cela, on adhère inconsciemment aux idées d'Euclide. Le diagramme est donc une escroquerie, car ce que Bolyai et Lobachevsky proposaient, c'était une nouvelle sorte de géométrie qui n'est pas en conformité avec la géométrie de bon sens d'Euclide. En fait, on peut considérer leur géométrie non euclidienne comme la géométrie sur la surface courbe de ce que l'on appelle une pseudo-sphère.

Les chemins les plus courts entre les points d'une pseudo-sphère jouent le même rôle que les droites dans la géométrie euclidienne. L'une des curiosités de cette géométrie non euclidienne, c'est que la somme des angles d'un triangle est inférieure à 180°. Cette géométrie s'appelle la géométrie hyperbolique.

Une autre alternative au cinquième postulat stipule que chaque droite qui passe par P coupe la droite Δ. Autrement dit, aucune droite qui passe par P n'est « parallèle » à Δ. Cette géométrie est différente de celle de Bolyai et de Lobachevsky, mais il s'agit néanmoins d'une géométrie authentique. Un modèle en est la géométrie sur la surface d'une sphère. Ici, les grands cercles (ces cercles qui ont la même circonférence que la sphère elle-même) jouent le rôle des droites dans la géométrie euclidienne. Dans cette géométrie non euclidienne, la somme des angles dans un triangle est supérieure à 180°. C'est ce que l'on appelle la géométrie elliptique que l'on associe au mathématicien allemand Bernhard Riemann qui en fit l'étude dans les années 1850.

La géométrie euclidienne, que l'on croyait être la seule vraie géométrie, ou, selon Emmanuel Kant, qui était « inhérente à l'esprit humain », était tombée de son piédestal. Elle était à présent une géométrie parmi d'autres, coincée entre la géométrie hyperbolique et la géométrie elliptique. Ses différentes versions furent unifiées sous une égide unique par Félix Klein en 1872. L'avènement de la géométrie non euclidienne stupéfia le monde des mathématiques et ouvrit la voie à la géométrie de la relativité d'Einstein (voir page 192). C'est la théorie de la relativité générale qui exige une nouvelle sorte de géométrie, la géométrie de l'espace-temps courbé, ou géométrie Riemannienne. L'explication de la chute des objets était maintenant donnée par cette géométrie non euclidienne, et non plus par la théorie de la force d'attraction gravitationnelle entre les objets définie par Newton. La présence d'objets massifs dans l'espace, comme la Terre et le Soleil, est à l'origine de la courbure de l'espace-temps. Une bille posée sur du caoutchouc peu épais provoque un petit renfoncement, mais essayez avec une boule de bowling et vous aurez une vraie déformation.

Cette courbure mesurée par la géométrie Riemannienne prédit comment les rais de lumière se courbent en présence d'objets massifs de l'espace. L'espace euclidien ordinaire, avec le temps comme composant indépendant, ne suffit pas pour rendre compte de la relativité générale. Une raison en est que l'espace euclidien est plat, donc sans courbure. Imaginez une feuille de papier étalée sur une table. On peut dire que la courbure est nulle en tout point de la feuille. Sous-jacent au concept de courbure se trouve un concept de courbure qui varie continuellement, tout comme la courbure d'un morceau de tissus froissé varie de point en point. De la même manière lorsque vous regardez dans un miroir déformant à la fête foraine, l'image que vous voyez dépend de l'endroit du miroir que vous regardez.

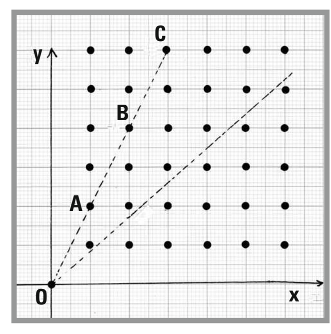
Il n'est pas étonnant que Gauss fut si impressionné par le jeune Riemann dans les années 1850 et alla jusqu'à suggérer que la « métaphysique » de l'espace serait révolutionnée par ses idées perspicaces.

l'idée clé
Et si des droites parallèles étaient sécantes ?

28 La géométrie discrète

La géométrie est l'un des arts les plus anciens. Pris au sens littéral, ce terme signifie mesure *(métrie)* de la Terre *(géo)*. En géométrie ordinaire, on étudie des droites continues et des figures que l'on peut se représenter comme des ensembles de points posés « les uns à côté des autres ». Les mathématiques discrètes traitent des nombres entiers par opposition aux nombres réels. La géométrie discrète peut impliquer un nombre fini de points et de droites appelés réseaux : le continu est remplacé par des éléments isolés.

Un réseau (ou une grille) est constitué d'un ensemble de points dont les coordonnées sont des nombres entiers. Cette géométrie, qui est à l'origine de problèmes intéressants, a des applications dans des domaines aussi variés que la théorie du codage et la conception d'expériences scientifiques.



Les points entiers du réseau

Prenons le cas d'un phare qui envoie un rayon de lumière. Imaginez que ce dernier a pour origine le point O et qu'il décrit un mouvement de va-et-vient entre l'horizontale et la verticale. On peut se demander quels rayons atteignent les points du réseau (qui pourraient représenter des bateaux amarrés et bien rangés le long du port).

L'équation du rayon à partir de l'origine est $y = mx$. C'est l'équation d'une droite de coefficient directeur m passant par l'origine. Si le rayon a pour équation $y = 2x$, alors il passe par le point de coordonnées $x = 1$ et $y = 2$ parce que ces valeurs satisfont l'équation. Si le rayon de lumière atteint un point de coordonnées $x = a$ et $y = b$, le coefficient directeur m est égal à la fraction b/a. Par conséquent, si m n'est pas rationnel ($\sqrt{2}$ par exemple), le rayon de lumière ne passe par aucun point du réseau.

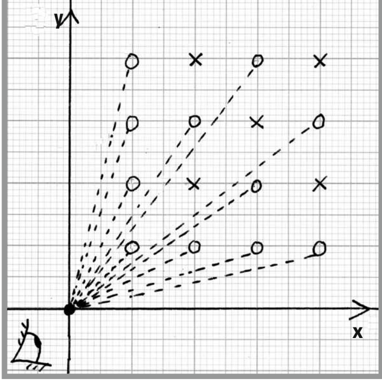
Le rayon de lumière d'équation $y = 2x$ passe par le point A de coordonnées $x = 1$ et $y = 2$, mais il ne passe pas par le point B de coordonnées $x = 2$ et $y = 4$

chronologie

1639
Pascal découvre le théorème qui porte son nom alors qu'il n'a que 16 ans.

1806
Brianchon découvre le dual du théorème de Pascal.

et tous les autres points placés « derrière » A (tels que *C*, de coordonnées $x = 3$ et $y = 6$ et *D* de coordonnées $x = 4$ et $y = 8$) sont dans l'obscurité. On pourrait imaginer que nous sommes postés à l'origine de manière à identifier les points visibles depuis cet endroit, et ceux qui ne sont pas éclairés.



Les points ○ « visibles » depuis l'origine et les points non visibles ×

On peut démontrer que les points de coordonnées $x = a$ et $y = b$ qui sont éclairés sont premiers entre eux. Ce sont des points dont les coordonnées n'ont aucun facteur commun, sauf le nombre 1, comme $x = 2$ et $y = 3$ par exemple. Les points situés à l'arrière sont leurs multiples, tels que $x = 4$ et $y = 6$, ou $x = 6$ et $y = 9$, et ainsi de suite.

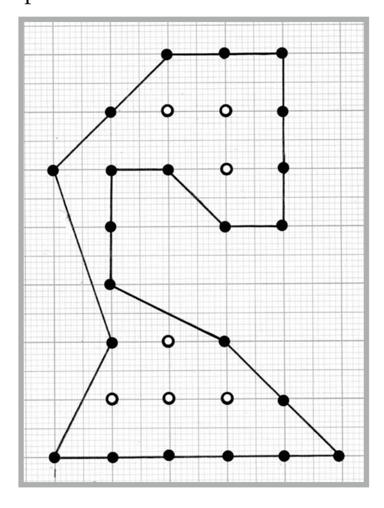
Le théorème de Pick Le mathématicien autrichien Georg Pick est célèbre pour deux raisons. Pour commencer, c'était un ami proche d'Albert Einstein et il ne fut pas étranger à la venue du jeune scientifique à l'Université Allemande de Prague en 1911. Ensuite, il écrivit un bref article, publié en 1899, sur la géométrie « réticulaire ». De ce travail de toute une vie qui a porté sur un grand nombre de sujets différents, on ne retient que le seul théorème de Pick, mais quel théorème captivant !

Le théorème de Pick permet de calculer l'aire à l'intérieur d'une figure à plusieurs côtés (un polygone convexe) que l'on forme en reliant les points dont les coordonnées sont des nombres entiers. C'est du flipper mathématique !

Pour trouver l'aire d'une figure, il faut compter le nombre de points entiers • sur le bord et le nombre de points entiers ° à l'intérieur de cette forme. Dans notre exemple, le nombre de points sur le bord est $b = 22$ et le nombre de points à l'intérieur est $c = 7$. C'est tout ce qu'il faut savoir pour utiliser le théorème de Pick qui s'énonce ainsi :

$$\text{aire} = b/2 + c - 1$$

Cette formule permet de trouver que l'aire est égale à 22/2 + 7 – 1 = 17. L'aire est de 17 unités d'aire. C'est aussi simple que cela. Le théorème de Pick peut s'appliquer à toutes les figures passant par des points entiers, la seule condition étant que le bord ne se recoupe pas lui-même.

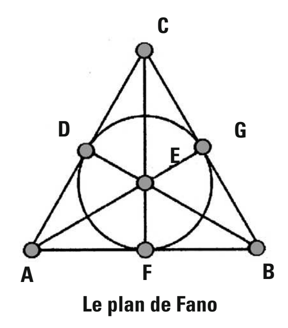


Un polygone ou figure à plusieurs côtés.

1846
Kirkman anticipe la découverte des Systèmes Triples de Steiner.

1892
Fano découvre le plan de Fano, exemple le plus simple de géométrie projective.

1899
Pick publie son théorème sur l'aire des polygones.



Le plan de Fano

Le plan de Fano La géométrie du plan de Fano fut découverte à peu près à la même époque que la formule de Pick, mais elle n'a rien à voir avec des mesures de quoi que ce soit. Nommée ainsi d'après le mathématicien Gino Fano qui ouvrit la voie dans l'étude de la géométrie finie, le plan de Fano est l'exemple le plus simple de géométrie « projective ». Elle ne comporte que sept points et sept droites.

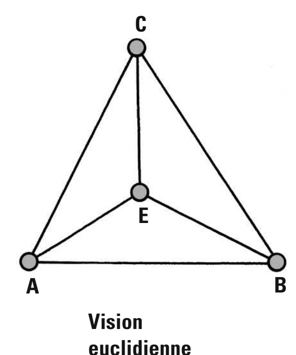
Les sept points sont appelés *A, B, C, D, E, F* et *G*. Il est facile de distinguer six des sept droites, mais où est la septième ? Les propriétés de la géométrie et la configuration du diagramme nous obligent à prendre pour septième droite *DFG*, puisque le cercle passe par *C, D, F* et *G*. Ce n'est pas un problème puisqu'en géométrie discrète, il n'est pas nécessaire que les droites soient « droites » au sens conventionnel.

Cette petite géométrie a de nombreuses propriétés. Par exemple :

- chaque paire de points détermine une droite qui passe par ces deux points,
- chaque paire de droites détermine un point qui se trouve sur ces deux droites.

Ces deux propriétés illustrent la dualité remarquable qui se produit dans les géométries de ce type. La deuxième propriété est en fait la première dont on a inversé les mots « point » et « droite », et de la même façon, la première propriété est la deuxième avec la même inversion de mots.

Si, dans une proposition quelconque, on inverse les deux mots et si l'on procède à de petits ajustements pour corriger le vocabulaire, on obtient une autre proposition vraie. La géométrie projective est très symétrique. La géométrie euclidienne ne l'est pas autant. Dans la géométrie euclidienne, nous avons des droites parallèles, c'est-à-dire des paires de droites qui ne se rencontrent jamais. On peut sans souci parler du concept de parallélisme dans la géométrie euclidienne. C'est impossible en géométrie projective où toutes les paires de droites se rencontrent en un point. Pour les mathématiciens, cela signifie que la géométrie euclidienne est une géométrie de type inférieur.



Vision euclidienne du plan de Fano

Si l'on enlève une droite mais aussi tous les points du plan de Fano, on revient dans la géométrie euclidienne non symétrique où existent des droites parallèles. Supposons que l'on enlève la droite « circulaire » *DFG* pour obtenir un diagramme euclidien.

Cette droite en moins, il en reste six : (*AB*), (*AC*), (*AE*), (*BC*), (*BE*) et (*CE*). Il y a maintenant des paires de droites « parallèles », à savoir (*AB*) et (*CE*), (*AC*) et (*BE*), (*BC*) et (*AE*). Les droites sont parallèles au sens où elles n'ont aucun point en commun, de la même manière que les droites (*AB*) et (*CE*).

Le plan de Fano fait figure d'icône en mathématiques pour toutes les idées et applications auxquelles il est lié. Il apporte une solution au problème des 15 pensionnaires

de Thomas Kirkman (voir page 167). Dans la théorie de la conception d'expériences, le plan de Fano se présente comme un exemple protéiforme, que l'on appelle un Système Triple de Steiner (STS). Étant donné un nombre n d'objets, un STS est une façon de les diviser en groupes de trois, de sorte que chaque paire prise dans les n objets se trouve dans un seul et unique groupe. Étant donnés sept objets A, B, C, D, E, F et G, les groupes du STS correspondent aux droites du plan de Fano.

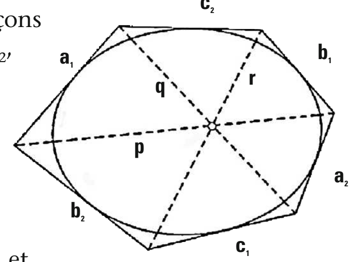
A	F	B
B	G	C
C	A	D
D	B	E
E	C	F
F	D	G
G	E	A

Une autre dualité en géométrie projective Le théorème de Pascal et le théorème de Brianchon se trouvent à la frontière qui sépare la géométrie continue de la géométrie discrète. Ces deux géométries sont différentes, mais néanmoins liées l'une à l'autre. Le théorème de Pascal fut découvert par Blaise Pascal en 1639 alors qu'il n'avait que 16 ans. Prenons une ellipse (voir page 89) et considérons six points sur cette ellipse que nous noterons A_1, B_1, C_1, A_2, B_2 et C_2. Nous appellerons P le point d'intersection des droites $(A_1 B_2)$ et $(A_2 B_1)$, Q le point d'intersection des droites $(A_1 C_2)$ et $(A_2 C_1)$ et R le point d'intersection des droites $(B_1 C_2)$ et $(B_2 C_1)$. Le théorème de Pascal stipule que les points P, Q et R sont alignés.

Le théorème de Pascal

Le théorème de Pascal est vrai quelle que soit la position des différents points disposés sur l'ellipse. On peut même remplacer l'ellipse par une autre conique, telle qu'une hyperbole, un cercle, une parabole, ou même deux droites parallèles (cette configuration s'appelle un « hexagramme mystique ») et le théorème est toujours vrai.

Le théorème de Brianchon fut découvert bien plus tard par le mathématicien et chimiste français Charles-Julien Brianchon. Traçons six tangentes à une ellipse, que nous appellerons a_1, b_1, c_1, a_2, b_2 et c_2. On définit les droites p, q et r comme suit : p est la droite passant par les points d'intersection de a_1 et b_2 et de a_2 et b_1 ; q est la droite passant par les points d'intersection de a_1 et c_2 et de a_2 et c_1 ; r est la droite passant par les points d'intersection de b_1 et c_2 et de b_2 et c_1. Le théorème de Brianchon stipule que les droites p, q et r sont concourantes.



Le théorème de Brianchon

Le théorème de Brianchon est le dual de celui de Pascal, et ces deux résultats donnent ainsi un autre exemple du principe de dualité en géométrie projective.

l'idée clé
Mise aux points individuels

29 Les graphes

Il existe deux types de graphes en mathématiques. À l'école, on trace des courbes qui montrent la relation entre deux variables *x* et *y*. Il existe une catégorie de graphes découverte plus récemment où des points sont reliés entre eux par des arêtes.

Königsberg est une ville de la Prusse Orientale bien connue pour ses sept ponts qui traversent le fleuve Pregolia. Ville de l'illustre philosophe Emmanuel Kant, elle est aussi, grâce à ses ponts, liée au célèbre mathématicien Leonhard Euler.

Au XVIII[e] siècle, on se posa une question étrange : était-il possible de faire le tour de Königsberg en passant une fois et une seule par chacun de ses ponts ? Il n'est pas nécessaire de revenir à notre point de départ au terme de cette promenade, mais en revanche, chaque pont doit être traversé une fois et une seule.

En 1735, Euler présenta la solution de ce problème à l'Académie Russe, solution qui est à l'origine de la théorie moderne des graphes. Dans notre représentation, l'île du milieu du fleuve est appelée *I* et les berges du fleuve *A*, *B*, et *C*. Pouvez-vous concevoir un itinéraire pour une promenade dominicale qui permette de traverser chaque pont une fois et une seule ? Prenez un crayon et essayez. La solution est de passer d'une représentation semi-abstraite à une représentation totalement abstraite. En procédant ainsi, on obtient un graphe constitué de points appelés « sommets » et de lignes appelées « arêtes » ou « arcs ». Les berges sont représentées par les sommets, et les ponts qui les relient par les arêtes. Peu importe qu'elles ne soient pas droites ou qu'elles soient de longueurs différentes. Ce n'est pas l'essentiel. Seules les connections nous intéressent.

Euler fit remarquer la chose suivante : à part au début et à la fin d'un tel itinéraire, à chaque fois que l'on traverse un pont, on doit

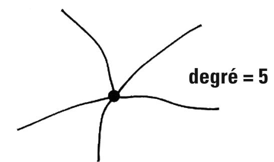
chronologie

1735
Euler résout le problème des ponts de Königsberg.

1874
Carl Schorlemmer établit un lien entre la chimie et les « arbres ».

pouvoir quitter la berge sur laquelle on se trouve par un pont qui n'a pas encore été traversé. En traduisant cette pensée en image abstraite, cela signifie que les arêtes adjacentes en un sommet doivent arriver par deux. À part les deux sommets qui représentent le début et la fin de la promenade, tous les ponts peuvent être traversés si et seulement si de chaque sommet part un nombre pair d'arêtes.

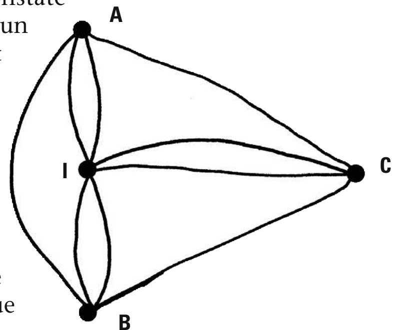
Le nombre d'arêtes adjacentes en un point s'appelle le « degré » du point.



Le théorème d'Euler stipule que

Les ponts d'une ville peuvent être traversés une fois et une seule si et seulement si tous les sommets du graphe sont de degré pair sauf éventuellement deux d'entre eux.

En regardant le graphe représentant Königsberg, on constate que chaque sommet est de degré impair. Cela signifie qu'un itinéraire qui permet de traverser chaque pont une fois et une seule est impossible à Königsberg. Si l'on modifiait la configuration du réseau de ponts, alors peut-être. Si l'on construisait un autre pont entre les îles *I* et *C*, les degrés de *I* et *C* seraient tous deux pairs. Cela signifie que l'on pourrait partir de *A* et terminer en *B*, après avoir traversé chaque pont une fois et une seule. Si l'on construisait un autre pont encore, cette fois entre *A* et *B* (voir le schéma de droite), on pourrait partir de n'importe quel endroit et y revenir parce que, dans ce cas, chaque sommet serait de degré pair.



Le théorème de la poignée de mains Si on nous demandait de dessiner un graphe contenant trois sommets de degré impair, nous aurions un problème. Essayez. On ne peut pas le faire parce que

Le nombre de sommets de degré impair d'un graphe quelconque doit être pair.

C'est le théorème de la poignée de main, premier théorème de la théorie des graphes. Dans un graphe quel qu'il soit, chaque arête a un début et une fin, ou en d'autres termes, il faut être au moins deux pour se serrer la main. Soit x (resp. y) le nombre de sommets de degré impair (resp. pair). Appelons N (resp. Nx ; Ny) la somme des degrés (resp. degrés impairs ; degrés pairs) des sommets du graphe.

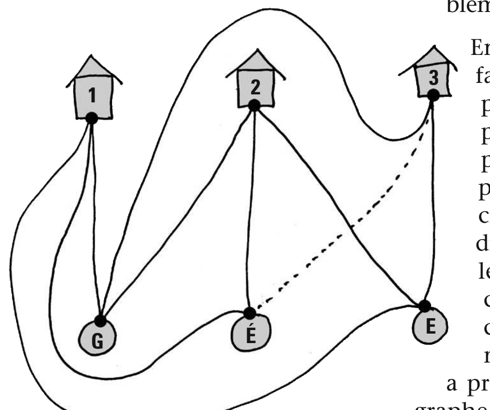
1930
Kuratowski prouve le théorème des graphes planaires.

1935
George Pólya développe des techniques algébriques d'énumération des graphes.

1999
Eric Rains et Neil Sloane développent l'énumération des structures arborescentes.

D'après ce qui précède, *N* est pair et il est clair que *N*y est pair également. De plus, on a *N*x + *N*y = *N* et, et donc *N*x = *N* – *N*y. Il s'ensuit que *N*x est pair. Cela implique que *x* est pair, car, sinon *N*x serait impair puisque la somme d'un nombre impair de degré impair donne un nombre impair.

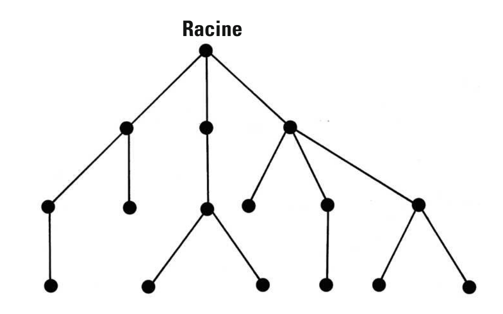
Graphes non planaires Le casse-tête des trois maisons est un classique. Imaginez trois maisons et trois bornes pour les alimenter en gaz, électricité, et eau. Il faut relier chacune des maisons à chacune des bornes, mais un problème se pose : aucun croisement ne doit se produire.



En réalité, c'est impossible, mais vous pouvez faire l'essai avec des amis qui ignorent tout du problème. Le graphe obtenu en reliant trois points à trois autres points de toutes les manières possibles (en utilisant neuf arcs seulement) ne peut pas être dessiné dans le plan sans que des croisements ne se produisent. Un tel graphe est dit non-planaire. Ce graphe des trois maisons et le graphe constitué de tous les arcs qui relient cinq points occupent tous deux une place particulière dans la théorie des graphes. En 1930, le mathématicien polonais Kazimierz Kuratowski a prouvé ce théorème surprenant selon lequel un graphe est planaire si et seulement si il ne contient aucun des deux graphes précédents.

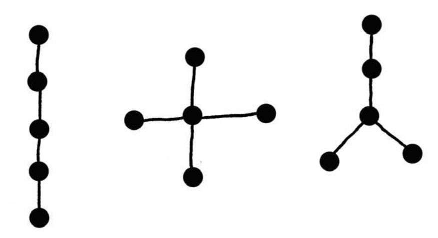
Les arbres Un « arbre » est une sorte particulière de graphe, très différente du graphe des trois maisons ou de celui des ponts de Königsberg. Dans le problème des ponts de Königsberg, il était possible de commencer en un point et d'y retourner par un chemin différent. Un tel trajet qui part d'un point pour y revenir s'appelle un cycle. Un arbre est un graphe qui n'a pas de cycle.

Un exemple connu de ce type de graphe se trouve dans la structure des répertoires des ordinateurs. Ils sont arrangés selon une hiérarchie constituée d'un répertoire



maître et de sous-répertoires qui s'en écartent. Parce qu'il n'y a pas de cycle, il n'y a aucun moyen de traverser d'une branche à l'autre autrement qu'en passant par le répertoire maître, manœuvre familière pour les utilisateurs d'ordinateurs.

Compter les arbres Combien d'arbres différents peut-on construire à partir d'un nombre spécifique de sommets ? Le problème de l'énumération des structures arborescentes a été traité par Arthur Cayley, grand mathématicien anglais du XIXe siècle. Il existe par exemple exactement trois types différents d'arbres comportant cinq points :



Cayley réussit à énumérer les structures arborescentes pour un nombre inférieur de points. Il s'arrêta aux arbres contenant moins de 14 points avant que la complexité du calcul ne soit trop grande pour un homme travaillant sans ordinateur. Depuis lors, les calculs ont progressé et nous en sommes maintenant à des arbres de 22 points. Il existe des millions de structures possibles dans ce cas.

Les recherches de Cayley avaient déjà des applications pratiques à son époque. Énumérer les arbres est utile en chimie, où le caractère distinctif de certains composés dépend de la manière dont les atomes sont arrangés dans leurs molécules. Les composés comportant le même nombre d'atomes arrangés différemment ont des propriétés chimiques différentes. L'utilisation de cette analyse permit de prédire « crayon en main » la présence de produits chimiques que des études en laboratoire pouvaient ensuite confirmer.

l'idée clé
Par les ponts et par les arbres

30 Le problème des quatre couleurs

Qui avait bien pu offrir à Tiny Tim, le héros de Charles Dickens, une boîte de quatre crayons de couleur et une carte muette de l'Angleterre pour Noël ? Peut-être le voisin cartographe, qui envoyait de temps en temps de petits cadeaux, ou bien Auguste De Morgan, ce mathématicien bizarre qui habitait dans le quartier, et qui échangeait parfois quelques mots avec le père de Tim. Ce n'était sûrement pas l'avare M. Scrooge.
La famille Cratchit habitait une modeste maison de Bayham Street, dans le quartier de Camden Town, au nord de l'université récemment ouverte où enseignait monsieur De Morgan. On découvrit l'origine du cadeau après les fêtes, lorsque le professeur leur rendit visite pour savoir si Tim avait colorié la carte.

De Morgan avait des idées bien arrêtées sur la manière de procéder : « Il faut que tu colories la carte de manière à ce que deux pays séparés par une frontière commune soient de deux couleurs différentes. »

« Mais je n'ai pas assez de crayons », répondit Tim sans réfléchir. De Morgan sourit et le laissa à sa besogne. Mais très récemment, l'un de ses étudiants, Frederick Guthrie, l'avait interrogé sur ce même sujet et avait fait référence à un procédé qui permettait de colorier l'Angleterre de quatre couleurs différentes seulement. Ce problème titilla son imagination mathématique.

Est-il possible de colorier une carte quelconque sans utiliser plus de quatre couleurs différentes, et de manière à ce que chaque région se différencie des régions adjacentes ? Les cartographes en eurent peut-être l'intime conviction pendant des siècles, mais est-il possible d'en apporter une preuve rigoureuse ? On peut se représenter toute carte, celle des comtés anglais, mais aussi la carte des États d'Amérique, celle des départements français, et même les cartes artificielles, comme un regroupement de régions et de frontières arbitraires. Il faut cependant plus de trois couleurs.

Examinons la carte des États de l'ouest de l'Amérique. Si l'on ne disposait que de bleu, de vert et de rouge, on pourrait commencer par colorier le Nevada et l'Idaho.

chronologie

1852
Guthrie, l'étudiant de De Morgan, énonce le problème des quatre couleurs.

1879
Kempe pense avoir résolu le problème des quatre couleurs.

1890
Heawood révèle les erreurs de la preuve de Kempe, et prouve un théorème des cinq couleurs.

Comme la couleur de départ n'a pas d'importance, nous prendrons du bleu pour le Nevada et du vert pour l'Idaho. Jusque-là, tout va bien. Ce choix oblige à colorier l'Utah en rouge, l'Arizona en vert, la Californie en rouge, et l'Oregon en vert. Autrement dit, l'Oregon et l'Idaho sont tous les deux coloriés en vert et ne peuvent donc pas être différenciés. Mais si l'on disposait d'une couleur supplémentaire, par exemple du jaune, nous pourrions l'utiliser pour colorier l'Oregon et tout irait bien. Ces quatre couleurs, le bleu, le vert, le rouge, et le jaune, seraient-elles suffisantes pour colorier n'importe quelle carte ? C'est ce que l'on appelle le problème des quatre couleurs.



Les États de l'ouest américain

La propagation du problème Dans les vingt années qui ont suivi la modélisation de ce problème par De Morgan qui en comprit toute la portée, il commença à se répandre dans la communauté mathématique européenne et américaine. Dans les années 1860, Charles Sanders Peirce, mathématicien et philosophe américain, pensait en avoir trouvé une preuve mais il ne reste aucune trace de son raisonnement.

Le problème prit davantage d'importance encore au XIXe siècle grâce à l'intervention de l'homme de science britannique Francis Galton. Voyant là un moyen de promouvoir la science, il usa de persuasion pour convaincre l'éminent mathématicien de Cambridge Arthur Cayley d'écrire un article sur le sujet en 1878. Malheureusement, Cayley fut contraint d'admettre qu'il n'avait pas réussi à obtenir une preuve mais observa qu'il suffisait de considérer les cartes cubiques uniquement (celles où trois pays exactement se rejoignent en un point). Cette contribution incita son étudiant Alfred Bray Kempe à chercher une solution. Pas plus d'un an plus tard, Kempe annonça avoir trouvé une preuve. Cayley le félicita chaleureusement, la preuve fut publiée, ce qui valut à Kempe son admission à la Royal Society de Londres.

Que se passa-t-il ensuite ? La preuve de Kempe était longue et techniquement très difficile à démontrer, et même s'il restait quelques sceptiques, elle fut généralement acceptée. Mais dix ans plus tard, surprise, Percy Heawood, de l'université de Durham, trouva un exemple de carte qui révélait une faille dans le raisonnement de Kempe. Il ne parvint pas à en apporter la preuve, mais Heawood montra toutefois que le problème des quatre couleurs n'était toujours pas résolu. Les mathématiciens n'avaient plus qu'à revenir à la planche à dessin et c'était aussi l'occasion pour quelque petit nouveau de se faire un nom. Utilisant certaines des techniques employées par Kempe, Heawood prouva un théorème des cinq couleurs selon lequel

1976

Appel et Haken prouvent le résultat général au moyen d'une preuve trouvée par ordinateur.

1994

La preuve par ordinateur est simplifiée mais reste une preuve trouvée par ordinateur.

toute carte pouvait recevoir cinq couleurs. Le résultat aurait été génial si l'on avait pu construire une carte qui ne pouvait pas se satisfaire de quatre couleurs. Les mathématiciens étaient bien embarrassés : fallait-il quatre ou cinq couleurs ?

Le problème de base des quatre couleurs concernait les cartes dessinées sur une surface plane ou sphérique. Qu'en était-il des cartes tracées sur une surface telle qu'un donut, surface intéressante pour les mathématiciens davantage pour sa forme que pour ses qualités gustatives. Heawood montra que sept couleurs étaient à la fois nécessaires et suffisantes pour colorier toute carte sur une telle surface. Il prouva même un résultat pour un donut à plusieurs trous (avec un nombre t de trous), dans lequel il comptait le nombre de couleurs suffisant pour colorier la carte, bien qu'il ne réussît pas à prouver que c'était le nombre minimum de couleurs nécessaires. Voici un tableau pour les premières valeurs de t de Heawood :

Le donut simple ou « tore »

Un tore à deux trous

Nombre de trous, t	1	2	3	4	5	6	7	8
Nombre minimum de couleurs, C	7	8	9	10	11	12	12	13

Et en général, $C = [1/2\ (7 + \sqrt{(1 + 48t)})]$. Les crochets désignent la partie entière du terme qu'ils encadrent. Par exemple, lorsque $t = 8$, C = [13,3107…] = 13. Heawood a démontré sa formule pour $t \geq 1$. Mais si l'on succombe à la tentation de prendre la valeur « interdite » $t = 0$, on obtient $C = 4$.

Le problème est-il résolu ? 50 ans plus tard, le problème, apparu en 1852, n'avait toujours pas été résolu. Au XXe siècle, l'intelligence de l'élite mathématique du monde entier se trouvait complètement désemparée.

On fit quelques progrès, tant et si bien qu'un mathématicien prouva qu'il suffisait de quatre couleurs pour représenter jusqu'à 27 pays sur une carte ; un autre fit mieux et affirma la même chose pour 31 pays, et un autre pour 35. Cette avancée par petites touches, si elle s'était poursuivie, aurait pu continuer à l'infini. En fait, les observations faites par Kempe et Cayley dans leurs tout premiers articles fournirent une meilleure méthode : les mathématiciens comprirent que l'on pouvait se contenter de vérifier la configuration de certaines cartes pour s'assurer qu'il suffisait de quatre couleurs. Mais le trop grand nombre de cartes posait problème puisqu'au début, il y en avait des centaines à vérifier. Cette vérification ne pouvait pas être faite à la main mais par chance, le mathématicien allemand Wolfgang Haken, qui avait travaillé sur le problème pendant de nombreuses années, réussit à s'assurer le concours du mathématicien et spécialiste en informatique Kenneth Appel. Des méthodes ingénieuses diminuèrent le nombre de configurations qui ne dépassèrent pas 1500. En juin 1976, au terme de nombreuses nuits blanches, le travail était accompli, et avec l'aide de leur fidèle ordinateur IBM 370, ils avaient résolu ce problème magnifique.

Le département de mathématiques de l'université de l'Indiana avait accompli un nouvel exploit. Ils remplacèrent le timbre à l'effigie du « plus grand nombre premier connu » par cette nouvelle que « quatre couleurs suffisent ». On était fier, dans l'Indiana, mais qu'attendait la communauté mathématique mondiale pour se réjouir ? Après tout, c'était un problème vénérable qu'un enfant comme Tiny Tim était en mesure de comprendre, mais qui avait quand même tourmenté certains des plus grands mathématiciens pendant plus d'un siècle.

On fit la fine bouche. Certains acceptèrent à contrecœur l'idée que le travail était terminé, mais beaucoup restèrent sceptiques. Le problème était que c'était un ordinateur qui avait donné la preuve, et cela sortait complètement du cadre traditionnel dans lequel s'inscrivent les preuves mathématiques. On s'attendait bien sûr à une preuve compliquée et longue, mais une preuve par ordinateur, c'était aller trop loin. Un problème se posait au niveau de la vérification de la preuve. Comment faire pour vérifier les milliers de lignes de code informatique dont elle dépendait ? On peut certainement faire des erreurs dans les codages informatiques. Et une erreur pouvait être fatale.

Mais ce n'est pas tout. Ce qui manquait vraiment, c'était l'émotion que procure la découverte. Comment lire cette preuve d'un bout à l'autre et apprécier toute la subtilité du problème, et comment éprouver ce sentiment d'émerveillement que suscite toujours la partie cruciale d'un raisonnement ? L'un des critiques les plus virulents se trouvait être le grand mathématicien Paul Hamos. Il pensait qu'une preuve par ordinateur était aussi crédible qu'une preuve apportée par une diseuse de bonne aventure même réputée. Mais beaucoup reconnaissent l'exploit, et il faudrait être courageux ou stupide pour gaspiller le temps précieux consacré à la recherche pour trouver un contre-exemple, à savoir une carte qui nécessiterait cinq couleurs. C'était peut-être possible avant Appel et Haken, mais pas après.

Après la preuve Depuis 1976, le nombre de configurations à vérifier a été réduit de moitié et dans le même temps, les ordinateurs sont devenus plus rapides et plus puissants. Cela dit, le monde mathématique attend toujours une preuve plus rapide qui s'inscrirait dans la tradition. En attendant, le théorème des quatre couleurs a engendré d'importants problèmes dans la théorie des graphes et a eu pour corollaire la remise en question de la nature même d'une preuve mathématique.

l'idée clé
Quatre couleurs suffisent

31 Les probabilités

Risque-t-il de neiger demain ? Quelle est la probabilité que demain je réussisse à prendre le premier train du matin ? Quelles sont vos chances de gagner au loto ? Les chances, la probabilité, le risque font partie du vocabulaire courant lorsque nous nous interrogeons sur l'avenir. Ce sont aussi les termes que l'on utilise en mathématiques dans la théorie des probabilités.

La théorie des probabilités est un sujet de grande importance. Elle est liée à la notion d'incertitude et constitue un ingrédient essentiel lorsqu'il s'agit d'évaluer des risques. Mais comment quantifier une théorie liée à l'incertitude ? Après tout, les mathématiques ne sont-elles pas une science exacte ?

Le vrai problème est de parvenir à une quantification de la probabilité.

Prenons l'exemple le plus simple qui soit, celui du lancer de pièce. Quelle est la probabilité d'obtenir « face » ? On pourrait immédiatement répondre que cette probabilité est de $^1/_2$ (que l'on écrit parfois sous la forme 0,5 ou 50 %). On suppose que la pièce n'est pas truquée, ce qui signifie qu'il y a autant de chances d'obtenir « face » que d'obtenir « pile », et donc que la probabilité d'obtenir « face » est égale à $^1/_2$.

Lorsqu'il s'agit de pièces, de balles dans des boîtes et de ce genre d'exemples « mécaniques », les choses sont relativement simples. Il existe deux grandes théories pour déterminer des probabilités. L'étude de la symétrie de la pièce fournit une première approche. Une autre approche est celle de la fréquence relative, où l'on mène l'expérience un très grand nombre de fois pour compter le nombre de « face ». Mais qu'entend-on par un grand nombre de fois ? Il n'est pas difficile de penser que le rapport entre le nombre de « face » et le nombre de « pile » est d'environ 50/50, mais cette proportion pourrait peut-être changer si l'on continuait l'expérience.

Comment donner une estimation raisonnable de la probabilité qu'il neigera demain ? Il y aura là encore deux solutions : il neigera ou il ne neigera pas, mais il n'est pas évident que ces deux solutions aient la même probabilité, comme c'était le cas avec la pièce. Pour estimer la probabilité qu'il neigera demain, il faut prendre en compte les conditions météorologiques au moment choisi et une foule d'autres facteurs. Malgré cela, il n'est pas possible de chiffrer cette probabilité avec exactitude. Il peut quand même s'avérer utile d'attribuer « un degré de certitude » qui indique

chronologie

Vers 1650
Pascal et Huygens posent les fondements de la théorie des probabilités.

1785
Condorcet applique la théorie des probabilités à l'analyse des systèmes de vote et de jury.

si la probabilité est faible, moyenne, ou élevée. En mathématiques, la probabilité se mesure sur une échelle qui va de 0 à 1. Un événement impossible a une probabilité de 0 et un événement certain une probabilité de 1. Une probabilité de 0,1 signifierait une faible probabilité, alors que 0,9 signifierait une forte probabilité.

Les origines des probabilités La théorie mathématique des probabilités s'est développée à partir des analyses de jeux de hasard effectuées par Blaise Pascal, Pierre de Fermat et Antoine Gombaud (aussi connu sous le nom de Chevalier de Méré) au XVIIe siècle. Un jeu tout simple les laissait perplexes. Le problème du Chevalier de Méré est le suivant : quel est l'événement le plus probable, obtenir un 6 en quatre jetés de dé, ou obtenir un double 6 en vingt-quatre lancers de deux dés ? Sur quel événement seriez-vous prêt à parier ?

À l'époque, on pensait que la solution la plus sage était de parier sur le double 6 en raison du nombre plus important de lancers autorisé. Cette opinion largement répandue fut anéantie lorsque l'on se lança dans l'analyse des probabilités. Voici comment il faut s'y prendre.

Jetez un dé : la probabilité de ne pas obtenir de 6 en un seul lancer est de 5/6. En quatre lancers, elle serait de 5/6 × 5/6 × 5/6 × 5/6, soit $(5/6)^4$. Comme les résultats des lancers n'ont aucune influence les uns sur les autres, ils sont dits « indépendants ». Il s'ensuit que l'on peut multiplier les probabilités. La probabilité d'obtenir au moins un 6 est donc :

$$1-\left(\frac{5}{6}\right)^4 = 0{,}517746\ldots$$

Jetez deux dés : la probabilité de ne pas obtenir de double 6 en un seul lancer est de 35/36 et en 24 lancers, elle est de $(35/36)^{24}$.

La probabilité d'obtenir au moins un double 6 est donc égale à

$$1-\left(\frac{35}{36}\right)^{24} = 0{,}491404\ldots$$

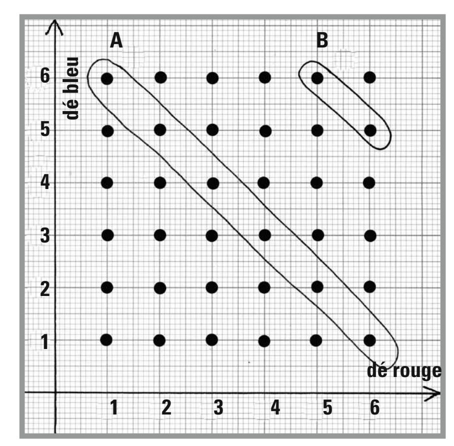
On peut aller un peu plus loin encore.

Jouer aux dés Cet exemple constitue le fondement du jeu de dés moderne qui se joue dans les casinos et dans les paris en ligne. Lorsqu'on lance deux dés distincts (un rouge et un bleu), il y a 36 résultats possibles que l'on peut noter sous la forme de couples (x,y), et que l'on peut représenter par 36 points placés dans un repère : c'est ce que l'on appelle « l'univers des possibles ».

1812
Laplace publie *Théorie analytique des probabilités*, ouvrage en deux volumes.

1912
Keynes publie un *Traité sur les probabilités* qui influence ses théories de l'économie et des statistiques.

1933
Kolmogorov pose les axiomes de la théorie des probabilités.



Univers des possibles (pour 2 dés)

Considérons « l'événement » A qui consiste à obtenir une somme de 7 avec les dés. Six combinaisons peuvent donner ce résultat, et on peut donc décrire l'événement comme suit :

$$A = \{(1,6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}$$

On l'entoure ensuite dans le diagramme. La probabilité de l'événement A est de 6 sur 36, ce qui peut s'écrire $P(A) = 6/36 = 1/6$. Si l'événement B consiste à obtenir une somme de 11 avec les dés, on a $B = \{(5, 6), (6, 5)\}$ et $P(B) = 2/36 = 1/18$.

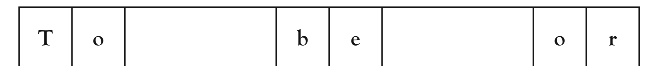
Au jeu du lancer de dés, qui se joue avec deux dés que l'on lance d'un bout à l'autre d'une table, on peut perdre ou gagner dès le premier lancer, mais dans certains cas, tout n'est pas perdu et on peut effectuer un deuxième lancer. On gagne au premier lancer si l'un des événements A ou B se produit : c'est ce que l'on appelle un « naturel ». Comme les événements A et B sont incompatibles (c'est-à-dire qu'ils n'ont aucun élément en commun), la probabilité d'obtenir un naturel s'obtient en additionnant les probabilités individuelles, 6/36 + 2/36 = 8/36. On perd dès le premier lancer si l'on obtient 2, 3 ou 12 (on appelle cela jouer un « craps »). Avec un calcul comme ci-dessus, la probabilité de perdre dès le départ est égale à 4/36. Si l'on obtient une somme de 4, 5, 6, 8, 9 ou 10, on lance les dés à nouveau et la probabilité de réussir est de 24/36 = 2/3.

Dans le monde des joueurs, on parle de cotes et non de probabilités. À ce jeu de dés, chaque fois que l'on joue 36 parties, on gagne 8 fois en moyenne au premier lancer et on perd 28 fois. Les chances de perdre au premier lancer sont donc de 28 contre 8, soit 3,5 contre 1.

Le singe sur une machine à écrire Alfred est un singe qui vit dans le zoo du coin. Il a une vieille machine à écrire toute cabossée avec 26 touches pour les lettres de l'alphabet, une touche pour le point, une pour la virgule, une pour le point d'interrogation et une pour faire les espaces, soit 30 touches au total. Il est assis dans un coin tout empreint de ses ambitions littéraires, mais sa méthode de travail est curieuse car il tape sur les touches au hasard.

Quelle que soit la suite de lettres qu'il tapera, elle aura une probabilité non nulle de se produire. Il y a donc une probabilité qu'il retranscrive les pièces de Shakespeare au mot près. Plus que cela, il y a une probabilité (plus faible cependant) qu'il enchaîne avec une traduction en français, puis en espagnol et pour finir, en allemand. On pourrait, pour le plaisir, prendre en compte la probabilité qu'il poursuive avec les poèmes de William Wordsworth. La probabilité est très faible, mais elle n'est certainement pas nulle. C'est là le point essentiel. Voyons combien de temps il lui faudrait pour taper le monologue de Hamlet à partir

des premiers mots « To be or ». On imagine 8 cases qui contiennent les 8 lettres, espaces inclus.



T	o		b	e		o	r

Le nombre de possibilités pour la première position est de 30, pour la seconde 30 également, et ainsi de suite. On peut remplir les 8 cases de $30 \times 30 \times 30 \times 30 \times 30 \times 30 \times 30 \times 30$ manières possibles. La probabilité qu'Alfred obtienne « To be or » est de 1 sur $6{,}561 \times 10^{11}$. Si Alfred tape à un rythme d'une touche par seconde, on peut s'attendre à ce qu'il tape « To be or » en 20 000 ans, ce qui en ferait un primate d'une longévité exceptionnelle. Alors, n'allez pas jusqu'à parier qu'il retranscrira les œuvres complètes de Shakespeare. Alfred produira des absurdités telles que « xo,h ?yt ? » les trois quarts du temps.

Comment la théorie s'est-elle développée ? Lorsque la théorie des probabilités est appliquée, les résultats peuvent être controversés, mais au moins, la charpente mathématique est bien solide. En 1933, Andrey Nikolaevich Kolmogorov fit un travail majeur en posant les bases axiomatiques des probabilités, tout comme Euclide qui avait défini les principes de la géométrie deux mille ans plus tôt.

Les probabilités se définissent selon les axiomes suivants :

1. la probabilité de l'ensemble de tous les résultats possibles est de 1 ;
2. la probabilité d'un événement a une valeur comprise entre 0 et 1 ;
3. lorsque les événements sont incompatibles, on peut additionner leurs probabilités.

À partir de ces axiomes, exprimés en termes techniques, découlent les propriétés mathématiques des probabilités. Le concept de probabilité peut être largement appliqué. Notre vie moderne ne peut pratiquement plus s'en passer que ce soit dans les analyses de risques, le sport, la sociologie, la psychologie, l'ingénierie, la finance, etc. La liste est interminable. Qui aurait pu penser que les problèmes de jeux de hasard qui ont lancé ces idées au XVIIe siècle engendreraient une discipline si vaste ? Quelle en était la probabilité ?

l'idée clé
Le système secret du joueur

32 La théorie de Bayes

On ne sait pas grand-chose des premières années du Révérend Thomas Bayes. Né probablement en 1702 dans le sud-est de l'Angleterre, ce pasteur non conformiste acquit aussi une solide réputation de mathématicien qui lui permit de se faire élire à la Royal Society de Londres en 1742. Son célèbre ouvrage intitulé *Essai pour résoudre un problème dans la doctrine des risques* fut publié en 1763, deux ans après sa mort. Il y donnait une formule pour trouver des probabilités *a posteriori*, ou probabilités « inverses », créant ainsi un concept central dans la philosophie bayésienne, celui de probabilité conditionnelle.

Thomas Bayes a donné son nom aux Bayésiens dont les méthodes s'opposent à celles des statisticiens traditionnels qualifiés de « fréquentistes ». Les fréquentistes ont une approche des probabilités qui repose sur des données numériques solides. L'approche bayésienne est fondée sur la célèbre formule de Bayes et sur le principe selon lequel des degrés subjectifs de croyance peuvent avoir valeur de probabilité mathématique.

La probabilité conditionnelle Imaginons que le fringant Dr Why ait pour mission de diagnostiquer la rougeole chez ses patients. La présence de boutons est un indicateur utilisé pour détecter la maladie mais le diagnostic n'est pas simple. Un patient peut avoir la rougeole sans avoir de bouton et à l'inverse, des patients peuvent présenter des boutons sans avoir contracté la maladie. La probabilité qu'un patient ait des boutons sachant qu'il a la rougeole est une probabilité conditionnelle. Les Bayésiens utilisent un trait dans leurs formules pour signifier « sachant que », et l'on écrit donc :

$$P \text{ (un patient a des boutons/le patient a la rougeole).}$$

Cette formule signifie la probabilité qu'un patient ait des boutons sachant qu'il a la rougeole. La valeur de P (un patient a des boutons/le patient a la rougeole) n'est pas la même que P (le patient a la rougeole/le patient a des boutons). Ces probabilités

chronologie

1763
Publication de l'essai de Bayes sur les probabilités.

1937
De Finetti défend la probabilité subjective comme une alternative à la théorie de la fréquence.

sont « inverses » l'une de l'autre. La formule de Bayes permet de calculer une probabilité à partir de l'autre. Ce dont les mathématiciens raffolent, c'est utiliser des notations pour représenter des choses. Appelons donc A l'événement « avoir la rougeole » et B l'événement « avoir des boutons ». L'événement $\overline{A}$ est l'événement « ne pas avoir la rougeole » et $\overline{B}$ est l'événement « ne pas avoir de boutons ». Un diagramme de Venn en donne une bonne représentation.

	B	$\overline{B}$	
A	x		a
$\overline{A}$			
			N

Représentation du problème des boutons et de la rougeole par un diagramme de Venn

Ce diagramme indique au Dr Why que x patients ont à la fois la rougeole et des boutons, a patients ont la rougeole, et qu'il y a N patients en tout. Ce diagramme nous montre que la probabilité qu'un patient ait à la fois la rougeole et des boutons est simplement de x/N, alors que la probabilité qu'un patient ait la rougeole est de a/N. La probabilité conditionnelle, la probabilité qu'un patient ait des boutons sachant qu'il a la rougeole, probabilité qui s'écrit $P(B/A)$, est de x/a. S'il réunit toutes ces informations, le Dr Why peut trouver la probabilité qu'un patient ait à la fois la rougeole et des boutons :

$$P(A \cap B) = \frac{x}{N} = \frac{x}{a} \times \frac{a}{N}$$

ou

$$P(A \cap B) = P(B/A) \times P(A)$$

et de la même façon

$$P(A \cap B) = P(A/B) \times P(B)$$

La formule de Bayes La mise en équation des expressions pour $P(A \cap B)$ donne la formule de Bayes, qui établit la relation entre la probabilité conditionnelle et son « inverse ». Le Dr Why aura une bonne idée de $P(B/A)$, c'est-à-dire de la probabilité qu'un patient ait des boutons sachant qu'il a la rougeole. Ce qui intéresse vraiment le Dr Why, c'est la probabilité conditionnelle de « l'inverse », à savoir sa capacité à évaluer la probabilité qu'un patient ait la rougeole sachant qu'il a des boutons. C'est donc du problème inverse qu'il s'agit, et c'est le type même de problème que Bayes traite dans son essai. Pour trouver les probabilités qui nous intéressent ici, il faut utiliser quelques nombres. Ils seront subjectifs mais l'important est de voir comment ils se combinent. La probabilité que des patients aient des boutons sachant qu'ils ont la rougeole est élevée, disons 0,9, ce qui donne au docteur une bonne idée de la situation. Le fringant

$$P(A/B) = \frac{P(A)}{P(B)} \times P(B/A)$$

La formule de Bayes

1950
Jimmy Savage et Dennis Lindley lancent le mouvement moderne Bayésien.

Dans les années 1950
Le terme Bayésien est employé pour la première fois.

1992
Fondation de la Société internationale pour l'analyse bayésienne (*International Society for Bayesian Analysis*).

docteur aura aussi une idée de la proportion de personnes dans la population qui ont la rougeole, disons 20 %, ce qui s'écrit $P(A) = 0{,}2$. Le seul renseignement dont nous avons besoin est $P(B)$, la proportion de personnes dans la population qui a des boutons. Maintenant, la probabilité qu'une personne ait des boutons est égale à la probabilité qu'une personne ait à la fois la rougeole et des boutons à laquelle s'ajoute la probabilité que quelqu'un n'ait pas la rougeole mais ait des boutons. À partir de nos relations clés, on obtient

$$P(B) = 0{,}9 \times 0{,}2 + 0{,}15 \times 0{,}8 = 0{,}3.$$

Avec ces valeurs, la formule de Bayes fournit :

$$P(A/B) = \frac{0{,}2}{0{,}3} \times 0{,}9 = 0{,}6$$

On en conclut que lorsqu'il examine les patients avec des boutons, le docteur fait un diagnostic correct de la rougeole dans 60 % des cas. Supposons maintenant que le docteur dispose de renseignements supplémentaires sur la souche du virus de sorte que la probabilité de détecter correctement la maladie augmente. Autrement dit, $P(B/A)$, la probabilité d'avoir des boutons à cause de la rougeole, passe de 0,9 à 0,95, et $P(B/A–)$, la probabilité que la présence de boutons ait une origine différente, passe de 0,15 à 0,1. Comment ce changement améliore-t-il son taux de détection de la rougeole ? Quelle est la nouvelle $P(A/B)$? Avec ces nouvelles données on a

$$P(B) = 0{,}95 \times 0{,}2 + 0{,}1 \times 0{,}8 = 0{,}27.$$

et la formule de Bayes entraîne

$$P(A/B) = \frac{0{,}2}{0{,}27} \times 0{,}95 = 0{,}704.$$

Le docteur peut maintenant détecter 70 % des cas grâce à ces renseignements supplémentaires. Si les probabilités passaient respectivement à 0,99 et 0,01 alors la probabilité de la détection, $P(A/B)$, passerait à 0,961 et ses chances de faire un diagnostic correct dans ce cas seraient donc de 96 %.

Les Bayésiens modernes Le statisticien traditionnel aurait peu à redire quant à l'utilisation de la formule de Bayes lorsque la probabilité peut être mesurée. Le point litigieux porte sur ces probabilités auxquelles on attribue des degrés de certitude, et que l'on qualifie parfois de probabilités subjectives.

Dans une cour de justice, on tranche parfois les problèmes de culpabilité ou d'innocence en ayant recours au principe de « l'équilibre des probabilités ». Pour le statisticien fréquentiste, parler de la probabilité qu'un prisonnier soit coupable d'un crime manque de sens. Il en va différemment avec le Bayésien pour lequel il n'est pas gênant de prendre en compte des impressions. Comment est-ce que cela marche ? Si nous devions utiliser la méthode de l'équilibre des probabilités pour décider de la culpabilité et de l'innocence, on pourrait voir que l'on peut jongler avec les probabilités. Voici un scénario possible.

Un juré vient d'entendre une affaire au tribunal et a décidé que la probabilité que l'accusé soit coupable est d'environ 1 sur 100. Au cours des délibérations, les jurés sont rappelés à la cour pour entendre d'autres preuves émanant de l'accusation. On a retrouvé une arme dans la maison de l'accusé, et l'avocat du ministère public affirme que la probabilité de la retrouver est de 0,95 si le prisonnier est coupable, mais s'il est innocent, la probabilité n'est plus que de 0,1. La probabilité de retrouver une arme dans la maison du prisonnier est donc beaucoup plus élevée si le prisonnier est coupable que s'il est innocent. Le problème pour le juré est donc de savoir comment modifier son opinion à la lumière de ce nouvel élément. On utilise notre notation à nouveau, et on note C l'événement « le prisonnier est coupable » et D l'événement « on détient de nouvelles preuves ». Le juré a estimé au départ que $P(C) = {}^1/_{100} = 0{,}01$. Cette probabilité s'appelle la probabilité antérieure. La probabilité de « réévaluation » $P(C/D)$ est la probabilité de la culpabilité après correction suite à l'apport d'une nouvelle preuve D. On l'appelle la probabilité postérieure. La formule de Bayes sous la forme

$$P(C/D) = \frac{P(D/C)}{P(D)} \times P(C)$$

montre l'idée d'une probabilité antérieure mise à jour par la probabilité postérieure $P(C/D)$. De la même façon que l'on a calculé $P(B)$ dans l'exemple médical, on peut calculer $P(D)$ et, en remplaçant ce résultat dans la formule de Bayes, on obtient :

$$P(C/D) = \frac{0{,}95}{0{,}95 \times 0{,}01 + 0{,}1 \times 0{,}99} \times 0{,}01 = 0{,}088.$$

Voilà qui est embarrassant pour le juré car l'estimation initiale de 1% de probabilité a presque atteint 9 %. Si l'accusation était allée plus loin en déclarant que la probabilité de trouver l'arme compromettante était d'au moins 0,99 si le prisonnier est coupable, mais seulement de 0,01 % s'il est innocent, alors, en reprenant la formule de Bayes, notre juré devrait réviser son opinion et la faire passer de 1 % à 50 %.

L'utilisation de la formule de Bayes dans de telles situations a fait l'objet de critiques. Le reproche principal concerne la manière dont on obtient la probabilité antérieure. L'analyse de Bayes présente quand même l'avantage de procurer une méthode qui permet de traiter les probabilités subjectives puis de les réviser en prenant appui sur des preuves. La méthode Bayésienne a des applications dans des domaines aussi divers que la science, les prévisions météorologiques et la justice criminelle. Ses partisans mettent en avant sa rigueur et son aspect pratique lorsqu'il s'agit de traiter l'incertitude. Elle a effectivement de nombreux atouts.

l'idée clé
Réévaluation des certitudes à l'aide de preuves

33 Le problème des anniversaires

Imaginez que vous êtes est assis dans un bus et que vous n'avez rien d'autre à faire que de compter les passagers qui en descendent pour se rendre au travail au petit matin. Comme ces passagers n'ont probablement aucun lien entre eux, on peut supposer sans risque que leurs dates d'anniversaire sont réparties aléatoirement tout le long de l'année. Il y a 23 passagers au total, vous y compris. Ce n'est pas beaucoup, mais c'est assez pour affirmer qu'il y a plus d'une chance sur deux que deux passagers soient nés le même jour de l'année. En êtes-vous convaincu ? Ils sont des millions à en douter mais c'est pourtant absolument vrai. Même un expert en probabilités de la valeur de William Feller avait du mal à y croire.

Le bus est maintenant trop petit pour nos besoins, c'est pourquoi nous reprenons notre raisonnement dans une pièce très spacieuse. Combien devrons-nous rassembler d'individus dans cette pièce pour être sûrs que deux personnes sont nées le même jour de l'année ? On compte 365 jours dans une année (ne nous occupons pas des années bissextiles), et s'il y avait 366 personnes dans la pièce, deux d'entre elles au moins seraient nées le même jour de l'année. Il est impossible qu'elles soient toutes nées des jours différents de l'année.

C'est le principe des tiroirs de Dirichlet (appelé encore principe du trou de pigeon ou principe des boîtes) : s'il y a $n + 1$ chaussettes qui occupent n tiroirs, alors un tiroir contient nécessairement plus d'une chaussette. Avec 365 personnes, impossible de savoir de manière certaine si une date d'anniversaire est commune à deux personnes parce que les anniversaires pourraient très bien tomber chacun à une date différente de l'année. Cependant, si vous prenez 365 personnes de manière aléatoire, ce serait alors extrêmement improbable, et la probabilité que deux personnes ne partagent pas la même date d'anniversaire serait extrêmement faible. Même avec seulement 50 personnes dans la pièce, il y a 96,5 % de chance que deux personnes soient nées le même jour. Si l'on réduit encore le nombre de personnes, la probabilité que deux personnes soient nées le même jour de l'année diminue. Vingt-trois

chronologie

1654
Blaise Pascal pose les fondations de la théorie des probabilités.

1657
Christiaan Huygens écrit le premier ouvrage publié sur les probabilités.

1718
Abraham de Moivre publie *La doctrine de la chance*, suivie d'éditions révisées et complétées en 1738 et 1756.

est le nombre de personnes pour lequel la probabilité est juste supérieure à 50 %, et pour 22 personnes, la probabilité que deux personnes soient nées le même jour de l'année est juste inférieure à 50 %. Le nombre 23 est la valeur critique. La réponse au problème classique de l'anniversaire est surprenante, mais pour autant, ce n'est pas un paradoxe.

Pouvons-nous le prouver ? Comment s'en convaincre ? Prenons une personne au hasard. La probabilité qu'une autre personne soit née le même jour de l'année qu'elle est de 1/365 et donc la probabilité que ces deux personnes ne soient pas nées le même jour de l'année est de 1 moins ce résultat (soit 364/365). La probabilité qu'une autre personne encore choisie au hasard soit née le même jour de l'année que les deux premières est de 2/365, et donc la probabilité que cette personne ne soit pas née le même jour de l'année qu'aucune des deux autres est égale à 1 moins ce résultat (soit 363/365). La probabilité qu'aucune de ces trois personnes ne soit née le même jour de l'année est égale au produit de ces deux probabilités, soit $(364/365) \times (363/365)$, soit 0,9918.

Si l'on continue selon ce même principe pour 4, 5, 6, … personnes, on dénoue le paradoxe du problème de l'anniversaire. Lorsque l'on arrive à 23 personnes, une calculatrice simple nous donne une probabilité de 0,4927 qu'aucune personne ne soit née le même jour de l'année qu'une autre. La négation de « aucune personne n'est née le même jour de l'année qu'une autre » est « au moins deux personnes sont nées le même jour de l'année », et la probabilité est égale à $1 - 0,4927 = 0,5073$ ce qui est juste supérieur au résultat initial 1/2.

Si $n = 22$, la probabilité que deux personnes soient nées le même jour de l'année est de 0,4757, ce qui est inférieur à 1/2. La nature apparemment paradoxale du problème de l'anniversaire est liée au langage. On obtient une affirmation à propos de deux personnes nées le même jour de l'année mais on ne sait rien de ces deux personnes. On ignore tout de cette date commune d'anniversaire. Si M. Trevor Thomson, qui est né le 8 mars, se trouve dans la pièce, une question différente peut être posée.

Combien d'anniversaires coïncident avec celui de M. Thomson ? Pour ce problème, le calcul est différent. La probabilité que M. Thomson ne soit pas né le même jour de l'année qu'une autre personne est de 364/365, de sorte que la probabilité qu'il ne soit pas né le même jour qu'aucune des personnes présentes est de $(364/365)^{n-1}$. La probabilité que M. Thomson ne soit pas né le même jour de l'année que quelqu'un d'autre est donc de 1 moins ce résultat.

Si on effectue le calcul pour $n = 23$, cette probabilité n'est que de 0,061151 et il n'y a donc que 6 % de chances que quelqu'un d'autre soit né le 8 mars, comme

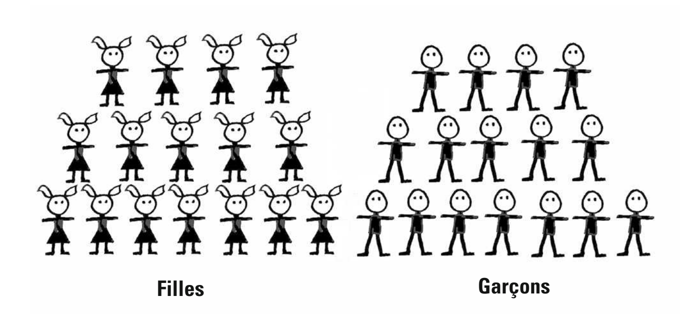
Dans les années 1920
Bose considère la théorie de la lumière d'Einstein comme un problème d'occupation.

1939
Richard von Mises propose le problème des anniversaires.

M. Thomson. Si l'on augmente la valeur de n, cette probabilité augmente. Mais il faut aller jusqu'à $n = 254$ (M. Thomson inclus) pour que la probabilité soit supérieure à 1/2. Pour $n = 254$ sa valeur est de 0,5005. C'est la valeur limite parce que $n = 253$ donne la valeur 0,4991 qui est inférieure à 1/2. Il faudra réunir 254 personnes dans la pièce pour avoir une chance supérieure à 1/2 que M. Thomson soit né le même jour de l'année que quelqu'un d'autre. Ce résultat correspond sans doute davantage à notre intuition que cette solution surprenante du problème classique de l'anniversaire.

D'autres problèmes d'anniversaire Le problème des anniversaires a été généralisé de diverses manières. Une approche est de considérer trois personnes nées le même jour de l'année. Dans ce cas, il faudrait 88 personnes pour qu'il y ait plus d'une chance sur deux que trois personnes soient nées le même jour. Les groupes sont proportionnellement plus importants si quatre, cinq personnes… doivent être nées le même jour. Dans un groupe de 1 000 personnes, par exemple, il y a plus d'une chance sur deux que 9 d'entre elles soient nées le même jour.

On a fait d'autres incursions dans le problème des anniversaires en examinant le problème des dates d'anniversaire proches. Dans ce type de problème, il faut qu'une personne soit née quelques jours avant ou après une autre. Il s'avère qu'il suffit de 14 personnes réunies dans une pièce pour avoir plus d'une chance sur deux d'être dans ce cas de figure.



Une variante de ce problème des anniversaires nécessite des outils mathématiques plus sophistiqués. Il s'agit du problème des garçons et des filles. Si une classe est composée d'un nombre égal de filles et de garçons, quel serait le groupe minimum pour lequel il y aurait plus d'une chance sur deux qu'un garçon et une fille soient nés le même jour ?

En fait, une classe de 32 élèves (16 filles et 16 garçons) serait le groupe minimum. On peut comparer ce résultat aux 23 personnes du problème classique des anniversaires.

En modifiant légèrement la question, on peut renouveler le problème (mais sa résolution est plus difficile). Supposons qu'une file d'attente se soit formée pour assister à un concert de Bob Dylan et que des gens viennent la rejoindre de manière aléatoire. Comme nous nous intéressons aux anniversaires, on ne tiendra pas compte de la possibilité que des jumeaux ou des triplés viennent ensemble. À leur entrée dans la salle de concert, on demande aux fans leur date d'anniversaire. Le problème

mathématique est le suivant : au bout de combien d'entrées aurons-nous deux personnes consécutives nées le même jour ? Un autre problème : combien de personnes entreront dans la salle de concert avant qu'une personne née le même jour que M. Trevor Morgan (le 8 mars) ne se présente ?

Le calcul de l'anniversaire suppose que les anniversaires soient uniformément répartis et que chaque anniversaire ait une chance égale de se produire pour une personne prise au hasard. Les résultats expérimentaux montrent que ce n'est pas tout à fait vrai (il y a plus de naissances en été) mais la réalité est suffisamment proche pour que l'on puisse lui appliquer ce résultat.

Les problèmes d'anniversaires sont des variantes des problèmes d'occupation où il s'agit pour les mathématiciens de réfléchir à la manière de placer des balles dans des cases. Dans le problème des anniversaires, le nombre de cases est de 365 (celles-ci sont assimilées à des anniversaires possibles) et les balles qui doivent être placées dans les cases sont des individus. Le problème peut être simplifié pour examiner la probabilité que deux balles tombent dans la même case. Pour le problème des filles et des garçons, les balles sont de deux couleurs.

Les mathématiciens ne sont pas les seuls à s'intéresser au problème des anniversaires. Satyendranath Bose porta son attention sur la théorie de la lumière d'Einstein, théorie qui repose sur les photons. Il quitta les voies traditionnelles de la recherche et posa la situation physique en termes de problème d'occupation. Pour lui, les cases n'étaient pas les jours de l'année comme dans le problème des anniversaires, mais les niveaux d'énergie des photons. Au lieu de répartir des gens dans des cases comme dans le problème des anniversaires, il répartissait des photons. Il existe de nombreuses applications des problèmes d'occupation dans d'autres sciences. En biologie, par exemple, la propagation des épidémies peut être modélisée en problème d'occupation : dans ce cas, les cases sont des régions géographiques, les balles, des maladies ; et le problème est de trouver la répartition des maladies.

D'étranges coïncidences se produisent dans la vie, mais seules les mathématiques fournissent une technique pour en calculer les probabilités. De ce point de vue, le problème classique des anniversaires n'est que la partie visible de l'iceberg et constitue une formidable introduction à ces mathématiques rigoureuses dont les applications sont d'importance.

l'idée clé
Le calcul des coïncidences

34 Les lois de probabilités

Ladislaus J. Bortkiewicz était fasciné par les tables de mortalité. Ce sujet n'avait rien de sinistre pour lui, mais il y voyait plutôt un champ d'investigation scientifique inépuisable. Bortkiewicz est connu pour avoir compté le nombre de cavaliers de l'armée prussienne tués par une ruade de cheval. Puis il y eut Frank Benford, physicien qui compta les premiers chiffres qui apparaissent dans différents types de données numériques pour voir combien elles contiennent de 1, de 2, et ainsi de suite. Enfin George Kingsley Zipf, qui enseignait l'allemand à Harvard, s'intéressait à la philologie et analysait les sorties de mots dans des textes donnés.

Tous ces exemples impliquent que l'on mesure les probabilités d'événements. Quelles sont les probabilités que x cavaliers reçoivent un coup de sabot mortel en une année ? Dresser la liste des probabilités pour chaque valeur de x s'appelle une distribution de probabilité ou, plus communément, une loi de probabilité. C'est aussi une loi de probabilité discrète parce que x ne prend que des valeurs isolées : les valeurs qui nous intéressent sont espacées les unes des autres. Trois ou quatre cavaliers prussiens peuvent être terrassés par un coup de sabot mortel mais pas 3,5. Comme nous le verrons plus loin avec la loi de Benford, on ne s'intéresse qu'à la sortie de « 1, 2, 3, …» et avec la loi de probabilité de Zipf, on peut trouver que le mot « it » apparaît en huitième position dans la liste des mots prépondérants en anglais, mais pas en 8,23^{e} position par exemple.

Vie et mort dans l'armée prussienne Bortkiewicz étudia dix corps de cavalerie pendant vingt ans, ce qui lui fournit des données pour 200 années d'un même corps. Il examina le nombre de décès (ce que les mathématiciens appellent la variable) et le nombre d'années écoulées avant d'atteindre ce nombre de décès. Il s'écoula par exemple 109 années sans aucun décès, alors qu'en une année, il y en eut quatre. Dans la caserne, le Corps C (par exemple) connut quatre décès en une seule année.

chronologie

1837
Siméon-Denis Poisson décrit la loi qui porte son nom.

1881
Newcomb découvre ce qui deviendra la loi de Benford.

1898
Bortkiewicz analyse les décès par ruade de cheval dans la cavalerie prussienne.

Comment le nombre de décès est-il réparti ? Recueillir ces renseignements fait partie du travail du statisticien, qui va sur le terrain relever des résultats. Bortkiewicz obtint les données suivantes :

Nombre de morts	0	1	2	3	4
Fréquence	109	65	22	3	1

Heureusement, les décès par ruade sont rares. La méthode la plus adaptée pour modéliser la fréquence des événements rares est ce que l'on appelle la loi de Poisson. Son utilisation aurait-elle permis à Bortkiewicz de prédire les mêmes résultats sans aller visiter les écuries ? La loi de Poisson stipule que la probabilité que le nombre de morts (que l'on appellera *x*) soit de valeur *r* est donnée par la formule de Poisson, où *e* ; 2,718… est ce nombre particulier associé à la « croissance » et dont il a précédemment été question (voir page 24) ; le point d'exclamation représente la factorielle, qui est ce nombre multiplié par tous les autres nombres entiers compris entre 1 et lui-même (voir page 26) ; la lettre grecque lambda, qui s'écrit λ, est le nombre moyen de morts. On a besoin de trouver cette moyenne sur les 200 années, et on multiplie donc 0 mort par 109 années (ce qui donne 0), 1 mort par 65 années (ce qui donne 65), 2 morts par 22 années (ce qui donne 44), 3 morts par 3 années (ce qui donne 9) et 4 morts par 1 année (ce qui donne 4), et on additionne toutes ces données (ce qui donne 122) et on divise par 200. Notre nombre moyen de morts par an est donc égal à 122/200 = 0,61.

$$e^{-\lambda}\lambda^{x}/x!$$

La loi de Poisson

On peut trouver les probabilités théoriques (que nous appellerons *p*) en utilisant la loi de Poisson avec les valeurs *r* = 0, 1, 2, 3 et 4. On obtient les résultats suivants :

Nombre de morts	0	1	2	3	4
Probabilités *p*	0,543	0,331	0,101	0,020	0,003
Nombre de morts attendus, $200 \times p$	108,6	66,2	20,2	4,0	0,6

La loi de Poisson semble bien adaptée pour traiter les données expérimentales réunies par Bortkiewicz.

Les premiers nombres Si l'on analyse les derniers chiffres de numéros de téléphone qui figurent dans une colonne d'annuaire, on pourrait s'attendre à ce que 0, 1, 2, …, 9 soient uniformément répartis. Ils apparaissent de manière aléatoire et les chances de sorties sont égales pour tout nombre. En 1938, le physicien Frank Benford a découvert que ce n'était pas vrai pour les premiers chiffres de certains ensembles de données. En fait, il a redécouvert une loi observée auparavant par l'astronome Simon Newcomb en 1881.

1938
Benford reformule la loi découverte par Newcomb.

1950
Zipf découvre une formule qui relie l'utilisation des mots au vocabulaire.

2003
La loi de Poisson est utilisée dans l'analyse des réserves de poissons dans l'océan Atlantique nord.

L'autre jour, j'ai fait une petite expérience. J'ai lu le taux de change des devises étrangères dans un quotidien national. Des taux de change tels que 2,119 indiquaient qu'il vous fallait 2,11 dollars pour acheter 1 livre sterling. De la même manière, il vous fallait 1,59 euro pour acheter 1 livre et 15,39 dollars de Hong Kong pour acheter 1 livre. Si l'on passe en revue les résultats de ces données, et si l'on note le nombre de sorties de la première décimale, on obtient le tableau suivant :

Première décimale	1	2	3	4	5	6	7	8	9	Total
Nombre de sorties	18	10	3	1	3	5	7	2	1	**50**
Pourcentage (%)	36	20	6	2	6	10	14	4	2	**100**

Ces résultats corroborent la loi de Benford selon laquelle, pour certaines classes de données, le chiffre 1 est la première décimale dont la fréquence de sortie est de 30 %, celle du nombre 2 est de 18 %, et ainsi de suite. Ce n'est certes pas la répartition uniforme observée dans les derniers chiffres des numéros de téléphone.

La raison pour laquelle un si grand nombre d'ensembles de données suivent la loi de Benford n'est pas évidente. Au XIXe siècle, lorsque Simon Newcomb observa l'usure des premières pages des tables logarithmiques, il aurait difficilement pu deviner l'importance que prendrait cette loi.

Les exemples où l'on peut repérer la loi de Benford incluent les résultats d'événements sportifs, les cours de la Bourse, les numéros des maisons, les populations, et la longueur des fleuves. Les unités de mesure importent peu : que les fleuves soient mesurés en mètres ou en miles ne change rien. La loi de Benford a des applications pratiques. Dès lors que l'on comprit que les données comptables suivaient cette loi, il devint plus facile de repérer les renseignements incorrects et ainsi de détecter les fraudes.

Les mots Parmi les nombreuses occupations de G. K. Zipf, figurait la pratique inhabituelle qui consistait à compter les mots. Dans la langue anglaise, les plus utilisés sont ces tout petits mots qui s'ordonnent ainsi :

Rang	1	2	3	4	5	6	7	8	9	10
Mot	the	of	and	to	a	in	that	it	is	was

Pour arriver à ce classement, on a pris un large échantillon parmi un éventail de productions écrites diverses et on a tout simplement compté les mots. Le mot le plus courant est placé au rang 1, le suivant au rang 2, et ainsi de suite. Il pourrait y avoir de légères différences dans la course à la popularité si l'on prenait un éventail de textes différents, mais sans plus.

Il n'est pas surprenant de voir que « *the* » est le mot le plus courant, et « *of* » le deuxième mot le plus utilisé. La liste continue et peut-être serez-vous intéressé par le fait que le terme « *among* » arrive en 500e position et « *neck* » en 1 000e position. Nous ne considérerons que les dix premiers mots. Si vous prenez un texte au hasard et comptez ces dix mots, vous trouverez à quelque chose près le même classement.

Ce qui est surprenant, c'est que les rangs influent sur le nombre réel de sorties des mots dans un texte. Le mot « *the* » apparaîtra deux fois plus que « *of* » et trois fois plus que « *and* », et ainsi de suite. Le nombre réel est donné par une formule célèbre. C'est une loi expérimentale que Zipf découvrit à partir de l'analyse de données. Selon la loi théorique de Zipf, le pourcentage de sorties du mot placé au rang r est donné par la formule :

$$\frac{k}{r} \times 100$$

où k ne dépend que de l'étendue du vocabulaire de l'auteur. Si un auteur maîtrisait tous les mots de la langue anglaise, qui en compte environ un million, selon certaines estimations, la valeur de k serait d'environ 0,0694. Dans la formule de la loi de Zipf, le mot « *the* » représenterait environ 6,94 % de tous les mots d'un texte. De la même façon, « *of* » en représenterait la moitié, c'est-à-dire environ 3,47 % de tous les mots. Un essai de 3 000 mots rédigé par un auteur aussi talentueux contiendrait par conséquent 208 sorties de « *the* » et 104 du mot « *of* ».

Pour les écrivains qui ne maîtrisent que 20 000 mots, la valeur de k passe à 0,0954, et il y aurait donc 286 sorties de « *the* » et 143 du mot « *of* ». Plus le vocabulaire est limité, plus il y a de sorties du mot « *the* ».

Voyance Que ce soit Poisson, Benford, ou Zipf, toutes ces lois nous permettent de faire des prédictions. Peut-être est-il impossible de prédire des événements avec 100 % de certitude, mais il vaut mieux connaître les lois de probabilités plutôt que de se lancer à l'aveuglette. En plus de ces trois lois, s'en ajoutent d'autres telles que la loi binomiale, la loi binomiale négative, la loi hypergéométrique, et bien d'autres encore, et le statisticien dispose ainsi d'une batterie d'outils efficaces pour analyser un vaste champ d'activités humaines.

l'idée clé
La prédiction de la quantité

35 La courbe de la loi normale

La courbe de la loi normale joue un rôle essentiel en statistique. On la considère comme l'équivalent de la droite en mathématiques. Elle a d'importantes propriétés mathématiques, mais si l'on entreprend d'analyser un bloc de données brutes, il est rare d'obtenir une courbe dont le tracé suit exactement celui d'une courbe de la loi normale.

La courbe de la loi normale est définie par une formule mathématique spécifique qui est à l'origine d'une courbe en cloche, la courbe de Gauss ; c'est une courbe qui dessine une bosse puis qui s'en écarte en s'abaissant doucement de chaque côté. L'intérêt de la courbe de la loi normale réside moins dans sa forme que dans la théorie dans laquelle elle s'inscrit, théorie qui a une longue histoire. En 1733, Abraham de Moivre, Huguenot français qui s'enfuit en Angleterre pour échapper à la persécution religieuse, créa cette courbe pour mener à bien son analyse des probabilités. Pierre Simon Laplace publia des résultats sur cette même courbe et Carl Friedrich Gauss l'utilisa en astronomie, domaine où elle est parfois appelée la loi Gaussienne.

Adolphe Quételet se servit de la courbe de la loi normale dans les études sociologiques qu'il publia en 1835 pour mesurer la dispersion d'un individu quelconque par rapport à « l'homme moyen ». D'autres expériences l'amenèrent à mesurer la taille des conscrits français et le périmètre thoracique de soldats écossais, en partant de l'hypothèse que ces mesures devaient suivre la courbe de la loi normale. À cette époque, on croyait fermement à cette notion de « normalité » ainsi définie et que l'on appliquait à la plupart des phénomènes.

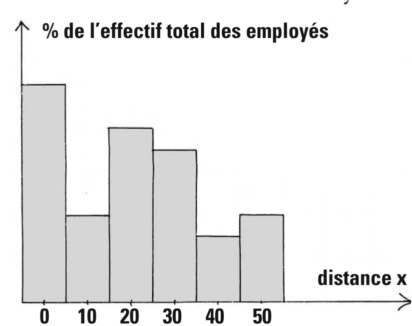
Le cocktail Supposons que Gabrielle se rende à un cocktail et que son hôte, Sébastien, lui demande si elle vient de loin. Elle se rend compte après coup que cette question est très utile dans ce genre d'occasion : elle peut être posée à tout le monde et appelle une réponse. Elle n'est pas embarrassante et permet de lancer la conversation si nécessaire.

chronologie

1733
De Moivre publie un travail sur la courbe de la loi normale qu'il présente comme une approximation de la loi binomiale.

1820
Gauss utilise la loi normale (ou loi de Gauss) en astronomie en tant que loi de l'erreur.

Le lendemain, à peine remise de ses agapes, Gabrielle se rend à son bureau en se demandant si ses collègues viennent de loin. Au restaurant de l'entreprise, elle apprend que certains collègues habitent à côté et que d'autres habitent à 75 km, et que les situations sont très variables. Profitant de sa fonction de Directrice des Ressources Humaines d'une très grande entreprise, elle ajoute une question au formulaire annuel adressé aux employés : « Quelle distance avez-vous parcourue pour vous rendre à votre travail aujourd'hui ? » Elle veut calculer la distance moyenne effectuée par le personnel de l'entreprise. Lorsque Gabrielle trace un histogramme des résultats, la répartition ne montre aucune forme particulière, mais il lui permet au moins de calculer la distance moyenne parcourue.



Histogramme de la distance parcourue par les collègues de Gabrielle pour se rendre à leur travail.

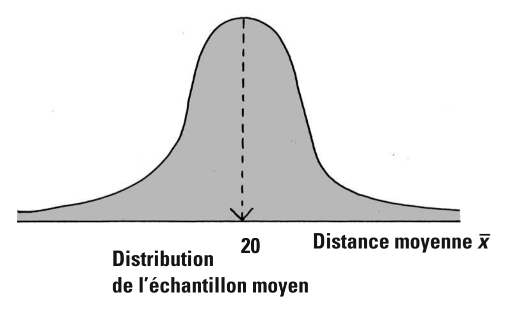
Cette moyenne est de 20 km. Les mathématiciens utilisent la lettre grecque mu, qui s'écrit μ, pour noter ce résultat, et donc ici, $\mu = 20$. La dispersion de la population se mesure à l'aide de l'écart type, qui s'écrit avec la lettre grecque sigma (σ). Si l'écart type est petit, les données sont concentrées autour de leur moyenne et la dispersion est faible, mais si l'écart type est grand, les données sont dispersées. L'analyste marketing de l'entreprise, qui a une formation de statisticien, montre à Gabrielle qu'elle aurait pu arriver à la même valeur, soit 20, en utilisant des échantillons plutôt que l'effectif total. Il n'était pas nécessaire de poser la question à tous les employés. Cette technique d'estimation repose sur le théorème central limite (TCL).

Prenons un échantillon aléatoire des membres du personnel de l'entreprise. Plus l'échantillon est important, mieux c'est, mais 30 employés font très bien l'affaire. En choisissant cet échantillon de manière aléatoire, on aura probablement des gens qui habitent près de l'entreprise, mais aussi des gens qui parcourent de longues distances. Lorsque l'on calcule la distance moyenne pour notre échantillon, l'effet des plus longues distances compensera celui des plus petites. Les mathématiciens utilisent la notation $\bar{x}$ pour désigner la moyenne des échantillons, notation qui se lit « x barre ». Dans le cas de Gabrielle, il est très probable que la valeur de $\bar{x}$ sera proche

1835
Quételet utilise la courbe de Gauss pour mesurer l'écart par rapport à l'homme moyen.

Dans les années 1870
La loi normale est ainsi baptisée.

1901
Aleksandr Lyapunov prouve le TCL en utilisant des fonctions caractéristiques.



de 20, la moyenne de la population. Bien qu'il soit peu probable que la moyenne de l'échantillon soit très petite ou très grande, cela pourrait toutefois arriver.

Le TCL est l'une des raisons pour lesquelles les statisticiens s'intéressent à la courbe de la loi normale. Il stipule que la répartition réelle des moyennes $\overline{x}$ de l'échantillon se rapproche d'une courbe de Gauss quelle que soit la répartition de x. Qu'est-ce que cela signifie ? Dans le cas de Gabrielle, x représente la distance entre le lieu de travail et $\overline{x}$ est la moyenne d'un échantillon. La répartition de x dans l'histogramme de Gabrielle n'a rien à voir avec une courbe en cloche, contrairement à la répartition de $\overline{x}$, et elle est centrée sur $\mu = 20$.

C'est la raison pour laquelle on peut utiliser la moyenne d'un échantillon $\overline{x}$ comme estimation de la moyenne de la population μ. La dispersion des moyennes des échantillons $\overline{x}$ constitue un avantage supplémentaire. Si la dispersion des valeurs x est donnée par l'écart type σ, la dispersion de $\overline{x}$ est égale à $\frac{\sigma}{\sqrt{n}}$ où n est la taille de l'échantillon choisit. Plus l'échantillon est grand, plus la courbe de Gauss est étroite, et meilleure est l'estimation de μ.

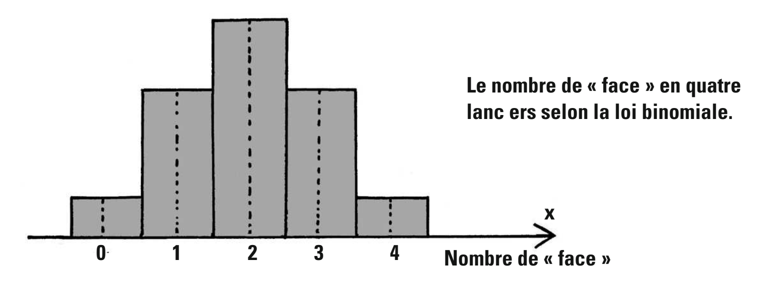
D'autres courbes du même type Faisons une expérience simple. Nous allons lancer une pièce quatre fois. La probabilité d'obtenir « face » à chaque fois que je lance la pièce est $p = 1/2$. Le résultat pour les quatre lancers peut être noté en utilisant *F* pour symboliser les « face » et *P* pour les « pile », en les classant selon leur ordre de sortie. Il y a en tout 16 sorties possibles. On peut par exemple obtenir trois « face » dans la sortie *PFFF*. En fait, on peut avoir quatre sorties qui donnent trois « face » (les autres étant *FPFF*, *FFPF*, *FFFP*) et la probabilité d'obtenir trois « face » est donc de 4/16 = 0,25.

Avec un petit nombre de lancers, les probabilités sont faciles à calculer et à présenter dans un tableau, et l'on peut aussi calculer la façon dont elles sont réparties. Le nombre de rangées de combinaisons peut être obtenu en utilisant le triangle de Pascal (voir page 52) :

Nombre de « face »	0	1	2	3	4
Nombre de combinaisons	1	4	6	4	1
Probabilité	0,0625	0,25	0,375	0,25	0,0625
	(= 1/16)	(= 4/16)	(= 6/16)	(= 4/16)	(= 1/16)

C'est ce que l'on appelle une loi binomiale. Elle se produit lorsqu'il y a deux sorties possibles (ici « pile » ou « face »). Ces probabilités peuvent être représentées à l'aide d'un histogramme constitué de rectangles dont les hauteurs et les surfaces donnent les sorties possibles.

Lancer la pièce quatre fois est un peu restrictif. Que se passe-t-il si on la lance un grand nombre de fois, 100 fois par exemple ? La loi binomiale peut s'appliquer lorsque $n = 100$, mais on peut en trouver une approximation utile à l'aide de la courbe en cloche, ce qui donne la moyenne $\mu = 50$ (puisque l'on pourrait s'attendre à 50 « face » lorsque l'on lance la pièce 100 fois) et la dispersion (l'écart type) de $\sigma = 5$. C'est ce que de Moivre découvrit au XVIIIe siècle.



Le nombre de « face » en quatre lanc ers selon la loi binomiale.

Pour les grandes valeurs de n, la variable x, qui mesure le nombre de succès, se rapproche de plus en plus de la courbe de Gauss. Plus la valeur de n est élevée, meilleure est l'approximation, et lancer la pièce 100 fois peut être considéré comme un grand nombre de fois. Imaginons maintenant que nous voulions connaître la probabilité d'obtenir entre 40 et 60 « face ». La surface A correspond à la région qui nous intéresse et nous donne la probabilité d'obtenir entre 40 et 60 « face », probabilité que nous écrivons $P(40 \leqslant x \leqslant 60)$. Pour trouver la valeur numérique réelle, on a recours à des tables mathématiques toutes faites, et on trouve ainsi $P(40 \leqslant x \leqslant 60) = 0{,}9545$. Autrement dit, la probabilité d'obtenir entre 40 et 60 « face » en 100 lancers de pièce est de 95,45 %, ce qui signifie que c'est fortement probable.

A

40 50 60 Nombre de « face »

Loi de probabilité pour le nombre de « face » obtenus en 100 lancers.

La surface restante est égale à 1 – 0,9545, soit 0,0455 seulement. Comme la courbe de Gauss est symétrique par rapport à son milieu, une moitié de la courbe donne la probabilité d'obtenir plus de 60 « face » en 100 lancers de la pièce. Cela ne représente qu'une probabilité de 2,275 %, ce qui est très faible. Si vous allez à Las Vegas, contentez-vous de regarder, c'est ce que vous avez de mieux à faire.

l'idée clé
L'ubiquité de la courbe en cloche

36 Données corrélées

Comment deux ensembles de données sont-ils corrélés ? Il y a un siècle, les statisticiens pensaient connaître la réponse. Corrélation et régression vont ensemble comme un cheval et son attelage, mais, comme eux, elles sont différentes et ont chacune leurs propres tâches à effectuer. La corrélation mesure le « degré d'association » entre deux quantités telles que le poids et la taille. La régression peut être utilisée pour prédire les valeurs d'une propriété (par exemple le poids) à partir d'une autre (dans ce cas, la hauteur).

La corrélation de Pearson Le terme corrélation fut introduit par Francis Galton dans les années 1880. C'est le terme « co-relation » qui fut d'abord utilisé, terme mieux choisi car plus explicite. Galton, gentilhomme anglais et homme de science de l'époque victorienne, voulait tout mesurer. C'est ainsi qu'il appliqua le concept de corrélation à ses études sur les paires de variables telles que la longueur des ailes et la longueur de la queue des oiseaux par exemple. Le coefficient de corrélation de Pearson, qui tient son nom de Karl Pearson, biographe et protégé de Galton, se mesure sur une échelle comprise entre -1 et $+1$. Si sa valeur numérique est élevée, par exemple $+0, 9$, on dit alors que les variables sont fortement corrélées. Le coefficient de corrélation mesure le comportement de données par rapport à une droite. S'il est proche de zéro, la corrélation est pratiquement nulle.

On recherche fréquemment la corrélation entre deux variables pour évaluer la force du rapport qui les unit. Prenons l'exemple de la vente de lunettes de soleil et examinons le rapport avec la vente de glaces. San Francisco serait l'endroit idéal pour mener notre étude, c'est pourquoi nous collecterons des données chaque mois dans cette ville. Si l'on place des points sur un graphe où l'axe des abscisses (axe horizontal) représente la vente de lunettes de soleil et l'axe des ordonnées (axe vertical) donne la vente de glaces, nous placerons chaque mois sur notre graphe un point de coordonnées (x, y) qui représente les deux données. Le point (3, 4) signifie par exemple que l'on a vendu pour 30 000 dollars de lunettes au mois de mai alors que l'on a vendu pour 40 000 dollars de glaces dans la ville au cours du même mois. On peut noter tous les points de coordonnées (x, y) pour une année complète sur un diagramme de diffusion. Pour cet exemple, la valeur du coefficient de corrélation de Pearson serait à peu près égal à $+0,9$ ce qui indique une forte corrélation. Les données ont tendance

chronologie

1806
Adrien-Marie Legendre étudie des données par la méthode des moindres carrés.

1809
Carl Friedrich Gauss utilise la méthode des moindres carrés pour résoudre des problèmes d'astronomie.

1885–1888
Galton introduit les concepts de régression et de corrélation.

à suivre une droite. Le coefficient est positif parce que la droite a un coefficient directeur positif : elle est orientée dans le sens nord-est.

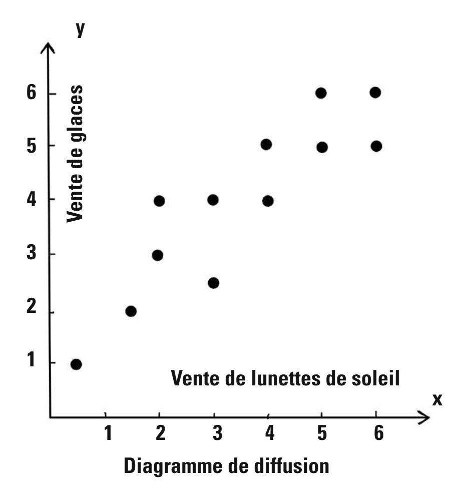


Diagramme de diffusion

Cause et corrélation Trouver une corrélation forte entre deux variables n'est pas suffisant pour affirmer que l'une est la cause de l'autre. Il existe peut-être une relation de cause à effet entre les deux variables mais il est impossible de l'affirmer en se fondant uniquement sur des preuves numériques. Lorsqu'il s'agit de traiter le problème du rapport entre la cause et la corrélation, on utilise habituellement le mot « association » et la prudence veut que l'on s'en tienne là.

Dans notre exemple, les ventes de lunettes et les ventes de glaces sont fortement corrélées. À mesure que la vente de lunettes augmente, le nombre de glaces vendues tend à augmenter. Il serait ridicule d'affirmer que les dépenses en lunettes de soleil sont à l'origine de l'augmentation de la vente de glaces. Dans une corrélation, une variable intermédiaire cachée peut opérer. Le lien entre les dépenses en lunettes et les dépenses en glaces, par exemple, est la conséquence directe des variations saisonnières (il fait chaud en période estivale et froid l'hiver). D'autre part, une mauvaise utilisation de la corrélation peut s'avérer dangereuse. Des variables peuvent être fortement corrélées sans qu'il y ait de rapport logique ou scientifique entre elles. Il pourrait y avoir une forte corrélation entre les numéros d'une maison et les âges combinés de ses occupants, mais il serait malencontreux d'y voir une quelconque signification.

La corrélation de Spearman La corrélation peut être utilisée à d'autres fins. Le coefficient de corrélation permet aussi de traiter des données rangées, c'est-à-dire des données pour lesquelles nous voulons connaître l'ordre de leurs premières valeurs numériques sans vouloir nécessairement connaître les autres valeurs numériques.

Nous avons parfois pour seules données des classements. Prenons Albert et Zac, deux juges de patinage intègres qui doivent évaluer la valeur artistique des patineurs lors d'une compétition. Leur évaluation est forcément subjective. Albert et Zac ont tous deux remporté des médailles aux jeux Olympiques et doivent maintenant juger le dernier groupe qui a été réduit à cinq compétiteurs : Anne, Béatrice, Charlotte, Dorothée et Elsa. Si Albert et Zac faisaient tous les deux le même classement, ce serait très bien, mais la vie n'est pas ainsi faite. D'un autre côté, on ne s'attendrait pas à ce qu'Albert les classe d'une manière et Zac d'une manière complètement

1896
Pearson publie ses contributions à la corrélation et à la régression.

1904
Spearman se sert du coefficient de corrélation des données rangées dans des études psychologiques.

différente. En fait, leurs classements seraient situés quelque part entre ces deux extrêmes. Albert les classerait de 1 à 5 en plaçant Anne en tête suivie d'Elsa, de Béatrice, de Charlotte et enfin de Dorothée qui viendrait en cinquième position. Zac classerait Elsa en première position, suivie de Béatrice, d'Anne, de Dorothée puis de Charlotte. Ces différents classements peuvent être résumés dans un tableau.

Patineuses	Classement d'Albert	Classement de Zac	Différence de classement (d)	d^2
Anne	1	3	–2	4
Elsa	2	1	1	1
Béatrice	3	2	1	1
Charlotte	4	5	–1	1
Dorothée	5	4	1	1
$n = 5$		Somme	**8**	

Comment peut-on mesurer le niveau d'accord entre les juges ? Le coefficient de corrélation de Spearman est l'instrument que les mathématiciens utilisent lorsqu'il s'agit de données rangées. Sa valeur est ici de +0,6, ce qui indique un niveau d'accord assez élevé entre Albert et Zac. Si l'on traite le classement des juges comme des points, on peut le représenter sur un graphe pour obtenir une représentation visuelle de la force de l'accord entre les juges.

$$1 - \frac{6 \times \sum d^2}{n \times (n^2 - 1)}$$

La formule de Spearman

La formule de ce coefficient de corrélation a été développée en 1904 par le psychologue Charles Spearman qui, comme Pearson, fut influencé par Francis Galton.

Régression linéaire Êtes-vous plus petit ou plus grand que vos deux parents, ou êtes vous quelque part entre les deux ? Si nous étions tous plus grands que nos parents, et si c'était le cas à chaque génération, alors un jour, la population pourrait être constituée de personnes de 3 mètres et plus, et cela ne se peut certainement pas. Si nous étions tous plus petits que nos parents, alors la population serait de plus en plus petite et c'est tout autant improbable. La vérité est ailleurs.

Zac
5
4
3
2
1
Albert
1 2 3 4 5

Mesure de l'accord entre deux juges

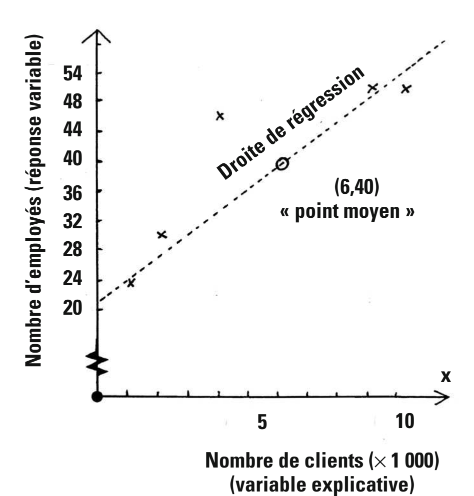
Francis Galton a mené des expériences dans les années 1880 dans lesquelles il comparait la taille de jeunes adultes avec celle de leurs parents. Pour chaque valeur de la variable x qui mesure la taille des parents (mesure qui combine la taille de la mère avec celle du père pour trouver la taille d'un parent « moyen »), il examina la taille de leur progéniture. Il s'agit ici d'un scientifique qui utilise une méthode expérimentale, et qui sortit donc papiers et crayons pour tracer des histogrammes représentant les données. Pour 205 parents moyens et leurs 928 rejetons, il trouva que la taille moyenne des deux ensembles était de 1 m 73, valeur qu'il appela la valeur moyenne. Il trouva que les enfants de très grands parents moyens étaient généralement plus

grands que la valeur moyenne mais pas aussi grands que leurs parents moyens, alors que les enfants plus petits étaient plus grands que leurs parents moyens, mais plus petits que la valeur moyenne. En d'autres termes, la taille des enfants régressait vers la valeur moyenne. C'est un peu comme les résultats exceptionnels du batteur Alex Rodriguez des New York Yankees. Sa moyenne offensive lors d'une saison exceptionnelle est susceptible d'être suivie par une moyenne inférieure la saison suivante, et pourtant globalement, elle sera toujours meilleure que la moyenne de tous les joueurs de la ligue. On dit que sa moyenne offensive a régressé vers la moyenne.

La régression est une technique puissante qui a de très larges applications. Supposons que, pour mener une étude, l'équipe de recherche opérationnelle d'une chaîne de vente au détail choisisse cinq de ses magasins, du petit magasin (1 000 clients par mois) jusqu'à la grande surface (10 000 clients par mois). L'équipe de recherche examine le nombre d'employés dans chacun des magasins. Ils projettent d'utiliser la régression pour estimer le nombre d'employés nécessaires dans les autres magasins.

Nombre de clients (1 000)	1	4	6	9	10
Nombre d'employés	24	30	46	47	53

Donnons une représentation de la situation sur un graphe, où *x* sera le nombre de clients (nous l'appelons la variable explicative) alors que *y* sera le nombre d'employés (appelé la réponse variable). C'est le nombre de clients qui explique le nombre d'employés nécessaires et non l'inverse. Le nombre moyen de clients dans les magasins est représenté au point d'abscisse 6 (6 000 clients) et le nombre d'employés au point d'ordonnée 40. La droite de régression passe toujours par le « point moyen », ici (6, 40). Il existe des formules pour calculer la droite de régression, cette droite qui convient le mieux aux données (aussi connue comme la droite des moindres carrés). Dans notre cas, une équation de la droite est $\hat{y} = 3{,}2x + 20{,}8$ et donc l'inclinaison est de 3,2 et elle est positive (elle est orientée dans le sens nord-est). La droite coupe l'axe vertical au point 20,8. Le terme $\hat{y}$ est l'estimation de la valeur *y* obtenue à partir de la droite. Si l'on veut donc connaître combien de personnes devraient être employées dans un magasin qui reçoit 5 000 clients par mois, on pourrait utiliser la valeur $x = 5$ dans l'équation de régression et l'on obtiendrait l'estimation $\hat{y} = 37$ employés, ce qui montrerait que la régression a bel et bien une utilité pratique.



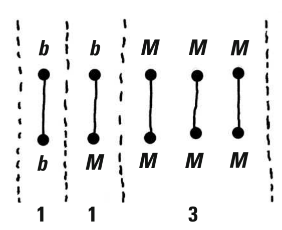
l'idée clé
L'interaction des données

37 La génétique

La génétique est une branche de la biologie, alors comment expliquer sa présence dans un livre de mathématiques ? En fait, ces deux matières se nourrissent l'une de l'autre et s'enrichissent mutuellement. La résolution de problèmes posés par la génétique nécessite un recours aux mathématiques, mais la génétique a aussi inspiré la création de nouvelles branches de l'algèbre. Gregor Mendel est le fondateur de cette science qui étudie les caractères héréditaires humains. Ces caractères, tels que la couleur des yeux, la couleur des cheveux, le daltonisme, le fait d'être gaucher ou droitier ainsi que le groupe sanguin, sont tous déterminés par les différentes versions possibles (ou allèles) d'un gène. Mendel disait que ces allèles sont transmis de manière indépendante à la génération suivante.

Comment l'allèle de la couleur des yeux peut-il être transmis à la génération suivante ? Fondamentalement, il y a deux allèles, *b* et *M* :

b est l'allèle des yeux bleus ;
M est l'allèle des yeux marron.



Population pour laquelle les proportions des génotypes bb, bM et MM sont de 20 %, 20 % et 60 %

Chez un individu, les allèles, présents par paires, constituent ses génotypes possibles, à savoir *bb*, *bM* et *MM* (parce que *bM* est identique à *Mb*). Une personne est porteuse de l'un de ces trois génotypes qui déterminent la couleur des yeux. Une population pourrait par exemple être constituée d'un cinquième de personnes au génotype bb, d'un autre cinquième au génotype *bM* et des trois cinquièmes restants au génotype MM. Exprimés en pourcentages, ces génotypes représenteraient 20 %, 20 % et 60 % de la population. Un diagramme permet de donner une représentation de ces génotypes.

L'allèle *M* des yeux marron est dominant, alors que l'allèle *b* des yeux bleus est récessif. Une personne dont le génotype est pur et qui possède donc les allèles identiques *MM* aura les yeux marron, mais il en ira de même pour une personne dont les allèles sont mixtes et qui a donc un génotype hybride *bM*, parce que *M* est dominant. Seul un individu au génotype pur *bb* aura les yeux bleus.

chronologie

1718
Abraham de Moivre publie *Théorie du hasard*.

1865
Mendel suggère l'existence de gènes et de lois de l'hérédité.

Un problème épineux se posa au début du XIX[e] siècle en biologie. Le nombre de personnes aux yeux marron finirait-il par s'imposer très largement face à celui des personnes aux yeux bleus qui s'éteindrait peu à peu ? Les yeux bleus allaient-ils disparaître à tout jamais ? Réponse : absolument pas.

La loi de Hardy-Weinberg L'explication a été donnée par la loi de Hardy-Weinberg, application des mathématiques élémentaires à la génétique. Elle explique comment, dans la théorie de l'hérédité de Mendel, un gène dominant ne supplante jamais complètement un gène récessif qui, lui, ne peut donc pas disparaître totalement.

G. H. Hardy était un mathématicien anglais pour qui les vraies mathématiques n'avaient pas d'applications pratiques, ce dont il se félicitait. Grand chercheur en mathématiques pures, il est toutefois probablement plus largement connu pour sa contribution à la génétique. Cette contribution prit au départ la forme de quelques formules mathématiques jetées au dos d'une enveloppe après un match de cricket. Wilhelm Weinberg venait d'un milieu différent. Médecin en Allemagne, il fut généticien toute sa vie. Il découvrit la loi au même moment que Hardy, vers 1908.

La loi s'applique à une large population au sein de laquelle les accouplements se forment de manière aléatoire. Il n'existe pas de préférences en matière d'accouplement, et ainsi les gens aux yeux bleus par exemple ne recherchent pas forcément des partenaires aux yeux bleus. L'enfant ainsi conçu reçoit un allèle de chacun de ses parents. Un génotype hybride *bM* qui s'accouple avec un hybride *bM* peut par exemple engendrer n'importe lequel des génotypes *bb, bM, MM*, mais un génotype *bb* qui va avec un *MM* ne peut qu'engendrer un hybride *bM*. Quelle est la probabilité qu'un allèle *b* soit transmis ? Si l'on compte le nombre d'allèles *b*, il y a deux allèles *b* pour chaque génotype *bb* et un *b* pour chaque génotype *bM*, ce qui donne, exprimé en fraction sur 10, un total de trois allèles *b* sur 10 (dans notre exemple d'une population dont les proportions des trois génotypes sont de 20 %, 20 % et 60 %). La probabilité de transmission de l'allèle *b* dans le génotype d'un enfant est donc de 3/10, soit 0,3. La probabilité de transmission d'un allèle *M* dans son génotype est de 7/10, soit 0,7. La probabilité que le génotype *bb* soit transmis à la génération suivante, par exemple, est donc de $0{,}3 \times 0{,}3 = 0{,}09$. L'ensemble complet des probabilités est résumé dans le tableau ci-dessous :

	b		*M*	
b	*bb*	$0{,}3 \times 0{,}3 = 0{,}09$	*bM*	$0{,}3 \times 0{,}7 = 0{,}21$
M	*Mb*	$0{,}3 \times 0{,}7 = 0{,}21$	*MM*	$0{,}7 \times 0{,}7 = 0{,}49$

Les génotypes hybrides *bM* et *Mb* sont identiques, et donc leur probabilité est de $2 \times 0{,}21 = 0{,}42$. Exprimés en pourcentage, les rapports des génotypes *bb*, *bM* et

1908
Hardy et Weinberg montrent pourquoi les gènes dominants ne supplantent pas les gènes récessifs.

1918
Fisher réconcilie la théorie de Darwin avec la théorie de Mendel de l'hérédité.

1953
La structure en double hélice de l'ADN est découverte.

MM dans la nouvelle génération sont de 9 %, 42 %, et 49 %. Parce que *M* est le facteur dominant, 42 % + 49 % = 91 % des individus de la première génération auront les yeux marron. Seuls les individus de génotype *bb* seront porteurs des caractères transmis par l'allèle *b*, et donc 9 % de la population seulement aura les yeux bleus.

La proportion initiale des génotypes était de 20 %, 20 % et 60 % et dans la nouvelle génération, elle est de 9 %, 42 % et 49 %. Que se passe-t-il ensuite ? Voyons ce qui se produit si une nouvelle génération est issue de cette première génération suite à d'autres accouplements aléatoires. La proportion des allèles *b* est égale à $0{,}09 + \frac{1}{2} \times 0{,}42 = 0{,}3$ et la proportion des allèles *M* est égale à $\frac{1}{2} \times 0{,}42 + 0{,}49 = 0{,}7$.

Ces résultats sont identiques aux probabilités de la transmission des allèles *b* et *M* obtenues précédemment. La proportion des génotypes *bb*, *bM* et *MM* dans la génération suivante est donc la même que pour la génération précédente, et le génotype bb qui donne les yeux bleus ne faiblit pas mais reste stable à 9 % de la population. Les proportions successives des génotypes pendant une suite d'accouplements aléatoires sont donc de 20 %, 20 %, 60 % → 9 %, 42 %, 49 % → … → 9 %, 42 %, 49 %. Ces résultats sont conformes à ce que stipule la loi de Hardy-Weinberg : après une génération, les proportions des génotypes restent constantes de génération en génération, de même que les probabilités de transmission.

Le raisonnement de Hardy Pour vérifier que la loi de Hardy-Weinberg fonctionne quelle que soit la population initiale et pas seulement lorsque les proportions sont de 20 %, 20 % et 60 % comme dans notre exemple, le mieux est de se reporter au raisonnement que Hardy envoya à l'éditeur du magazine américain *Science* en 1908.

Hardy commence avec la proportion initiale des génotypes *bb*, *bM* et *MM* qu'il appelle p, $2r$ et q et les probabilités de transmission $p + r$ et $r + q$. Dans notre exemple numérique (de 20 %, 20 %, 60 %), $p = 0{,}2$, $2r = 0{,}2$ et $q = 0{,}6$. Les probabilités de transmission des allèles *b* et *M* sont égales à $p + r = 0{,}2 + 0{,}1 = 0{,}3$ et $r + q = 0{,}1 + 0{,}6 = 0{,}7$. Que se passe-t-il si la distribution initiale des génotypes *bb*, *bM* et *MM* est différente et si l'on a par exemple au départ 10 %, 60 % et 30 % ? Comment la loi de Hardy-Weinberg fonctionne-t-elle dans ce cas ? On a alors $p = 0{,}1$, $2r = 0{,}6$ et $q = 0{,}3$ et les probabilités de transmission des allèles *b* et *M* sont respectivement $p + r = 0{,}4$ et $r + q = 0{,}6$. La proportion des génotypes de la génération suivante est donc de 16 %, 48 % et 36 %. Les proportions successives des génotypes *bb*, *bM* et *MM* après des accouplements aléatoires sont les suivants :

10 %, 60 %, 30 % → 16 %, 48 %, 36 % → … → 16 %, 48 %, 36 %

Les proportions se stabilisent après une génération, comme précédemment, et les probabilités de transmission de 0,4 et 0,6 restent constantes. Avec ces chiffres, 16 % de la population a les yeux bleus et 48 % + 36 % = 84 % a les yeux marron parce que *M* est dominant dans le génotype *bM*.

La loi de Hardy-Weinberg implique donc que les proportions des génotypes *bb*, *bM* et *MM* restent constantes de génération en génération quelle que soit la répartition

initiale des allèles dans la population. Le gène dominant *M* ne prend pas le dessus et les proportions des génotypes sont intrinsèquement stables.

Hardy insista sur le fait que son modèle n'était qu'approximatif. Sa simplicité et son élégance découlent de nombreuses hypothèses que l'on ne rencontre pas dans la vie réelle. La probabilité d'avoir une mutation de gène ou des changements dans les gènes eux-mêmes n'a pas été prise en compte, et la stabilité des proportions de transmission signifie que ce modèle ne peut rien nous apprendre sur l'évolution. Dans la vie réelle, un « glissement génétique » se produit et les probabilités de transmission des allèles ne sont pas toujours constantes. C'est ce qui est à l'origine des variations des proportions globales, variations qui sont elles-mêmes responsables de l'évolution des espèces.

La loi de Hardy-Weinberg réunit la théorie de Mendel, ou « théorie quantique » de la génétique, et la théorie de la sélection naturelle de Darwin. Il fallut attendre le génie de R. A. Fisher pour réconcilier la théorie de Mendel de l'hérédité avec la théorie du continu selon laquelle les caractères évoluent.

Jusqu'aux années 1950 il nous a manqué une compréhension physique du matériel génétique lui-même. Puis une grande avancée fut rendue possible par les travaux de Francis Crick, James Watson, Maurice Wilkins et Rosalind Franklin. On se servit d'acide désoxyribonucléique appelé ADN. Les mathématiques sont nécessaires pour modéliser la célèbre double hélice (ou paire de spirales enroulées autour d'un cylindre). Les gènes se trouvent sur des segments de cette double hélice.

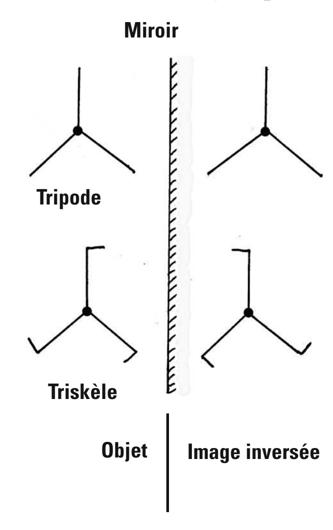
Les mathématiques sont indispensables pour étudier la génétique. À partir de la géométrie élémentaire des spirales d'ADN et de la loi potentiellement sophistiquée de Hardy-Weinberg, des modèles mathématiques ont été développés qui traitent de nombreux caractères (et pas seulement la couleur des yeux) tels que les différences sexuelles entre hommes et femmes ; on a aussi étudié le cas des accouplements non aléatoires. La science de la génétique a en outre renvoyé l'ascenseur aux mathématiques en suggérant de nouvelles branches de l'algèbre qui présentent un intérêt certain en raison de leurs propriétés mathématiques curieuses.

l'idée clé
Incertitude dans le pool génétique

38 Les groupes

Évariste Galois est mort dans un duel à l'âge de 20 ans, mais il a laissé derrière lui suffisamment d'idées pour occuper les mathématiciens pendant des siècles. Parmi celles-ci, figurait la théorie des groupes, constructions mathématiques que l'on peut utiliser pour quantifier la symétrie. Sans parler de son attrait artistique, la symétrie est l'ingrédient essentiel pour les scientifiques qui rêvent d'établir une théorie du tout. La théorie des groupes est le ciment qui unit ce « tout ».

La symétrie est partout présente autour de nous. On la trouve dans les vases grecs, les bâtiments et certaines lettres de l'alphabet. Il existe plusieurs sortes de symétrie : les principales sont la symétrie axiale (ou symétrie miroir, ou réflexion) et la rotation. Nous allons simplement examiner la symétrie à deux dimensions puisque tous les objets que nous étudierons se trouvent sur la surface plane de cette page.



La symétrie axiale Peut-on placer un miroir de sorte qu'un objet soit identique devant le miroir et dans le miroir ? Les mots SOS et NON sont symétriques par rapport au miroir, mais ce n'est pas le cas pour MAT et POT ; SOS devant le miroir est identique à SOS dans le miroir, alors que MAT devient TAM. Un tripode (figure à trois branches) possède une symétrie miroir, contrairement au triskèle (tripode dont les trois branches sont incurvées dans le même sens). Devant le miroir, le triskèle est orienté à droite, mais son image est orientée à gauche.

La rotation On peut aussi se demander s'il y a un axe perpendiculaire par rapport à la page, de sorte que l'on puisse faire pivoter l'objet sur cette page selon un angle donné et le faire ainsi revenir à sa position initiale. Le tripode et le triskèle restent inchangés par une certaine rotation. Le triskèle, qui signifie « trois jambes », est une forme intéressante. Orientée à droite, cette figure est le symbole de l'île de Man et apparaît également sur le drapeau de la Sicile.

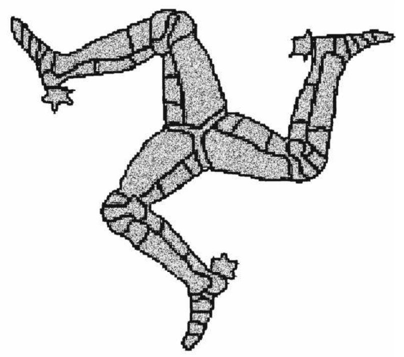
chronologie

1832
Galois propose l'idée de groupes de permutations.

1854
Cayley entreprend de généraliser le concept de groupe.

1872
Felix Klein inaugure un programme pour établir une classification de la géométrie en utilisant les groupes.

Si on lui fait subir une rotation de 120° ou de 240°, la figure coïncidera avec elle-même ; si vous fermez les yeux avant d'effectuer cette rotation, vous verrez le même triskèle en ouvrant les yeux après la rotation.



Le triskèle de l'île de Man

Ce qui est curieux avec cette figure à trois branches, c'est qu'aucune rotation du plan ne pourra jamais convertir un triskèle orienté à droite en triskèle orienté à gauche. Les objets pour lesquels l'image dans le miroir est différente de l'objet devant le miroir sont dits chiraux : ils paraissent identiques mais ne le sont pas. La structure moléculaire de certains composés chimiques peut exister sous la forme de figures en trois dimensions orientées à droite ou à gauche et sont donc de parfaits exemples d'objets chiraux. C'est le cas avec le limonène composé qui, sous une certaine forme, a un goût de citron, et sous une autre, un goût d'orange. La thalidomide est sous une certaine forme un remède efficace contre les nausées matinales de la grossesse mais sous une autre forme, elle a des conséquences tragiques sur le fœtus.

La mesure de la symétrie Dans le cas de notre triskèle, les opérations de base sont les rotations R d'angle 120° et S d'angle 240° (dans le sens des aiguilles d'une montre). La transformation I est celle qui fait effectuer au triangle une rotation d'angle 360°, c'est-à-dire qui ne lui fait subir aucune rotation. On peut créer un tableau à partir des combinaisons de ces rotations, de la même manière que l'on pourrait créer une table de multiplication.

Ce tableau est une table ordinaire de multiplication comportant des nombres, mais la différence est que l'on « multiplie » des symboles. Selon la convention la plus communément employée, la multiplication $R \circ S$ signifie qu'il faut d'abord faire tourner le triskèle dans le sens des aiguilles d'une montre à 240° avec S, puis de 120° avec R, ce qui donne une rotation d'angle 360°, comme si rien ne s'était passé. On peut l'écrire sous la forme $R \circ S = I$, résultat qui se trouve à la jonction de l'avant dernière ligne et de la dernière colonne du tableau.

$\circ$	I	R	S
I	I	R	S
R	R	S	I
S	S	I	R

Table de Cayley pour le groupe du triskèle

Le groupe symétrique du triskèle est constitué de I, R et S et la table de multiplication indique comment les calculer. Puisque le groupe contient trois éléments, sa taille (ou son « ordre ») est égale à 3. Cette table s'appelle aussi une table de Cayley (d'après le mathématicien Arthur Cayley, cousin éloigné de Sir George Cayley, pionnier de l'aviation).

1891

Evgraf Fedorov et Arthur Schönflies réalisent chacun de leur côté une classification des 230 groupes cristallographiques.

1983

La classification des groupes finis simples est achevée et le théorème énorme est prouvé.

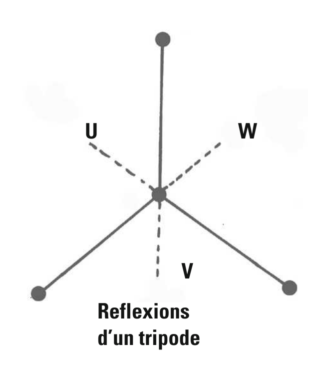
∘	*I*	*R*	*S*	*U*	*V*	*W*
I	*I*	*R*	*S*	*U*	*V*	*W*
R	*R*	*S*	*I*	*V*	*W*	*U*
S	*S*	*I*	*R*	*W*	*U*	*V*
U	*U*	*W*	*V*	*I*	*S*	*R*
V	*V*	*U*	*W*	*R*	*I*	*S*
W	*W*	*V*	*U*	*S*	*R*	*I*

Table de Caley pour le groupe du tripode

Comme pour le triskèle, il existe une rotation laissant le tripode fixe, mais il existe aussi une symétrie axiale, et donc un groupe de symétrie plus vaste. Nous appellerons *U*, *V* et *W* les réflexions selon les trois axes du miroir.

Le groupe de symétrie du tripode, qui est d'ordre 6, est composé des 6 transformations *I, R, S, U, V* et *W*. Sa table de multiplication est représentée ci-contre.

Une transformation intéressante s'obtient en composant deux réflexions par rapport à deux axes distincts, par exemple $U \circ W$ (où la réflexion *W* est appliquée en premier et est suivie de la réflexion U). On obtient une rotation d'angle 120° du tripode, et donc on a $U \circ W = R$. En revanche, l'opération $W \circ U = S$ donne une rotation d'angle 240°. En particulier, $U \circ W \neq W \circ U$. C'est une différence majeure entre la table de multiplication pour un groupe et une table de multiplication ordinaire avec des nombres.



Reflexions d'un tripode

Un groupe dans lequel l'ordre de composition des éléments n'a pas d'importance s'appelle un groupe abélien, du nom du mathématicien norvégien Niels Abel. Le groupe de symétrie du tripode est le plus petit groupe qui n'est pas abélien.

Les groupes abstraits Au cours du XXe siècle, l'algèbre classique a évolué vers l'algèbre abstraite dans laquelle un groupe est défini par certaines règles de base appelées axiomes. De ce point de vue, le groupe de symétrie du triangle devient un simple exemple de système abstrait. En algèbre, certains systèmes sont plus élémentaires qu'un groupe et nécessitent un nombre moins important d'axiomes ; d'autres systèmes plus complexes nécessitent davantage d'axiomes. Cependant, l'admirable concept de groupe est le système algébrique le plus impsortant de tous. Grâce à la méthode abstraite, on peut déduire les théorèmes généraux pour tous les groupes, et les appliquer, si nécessaire, à des groupes particuliers.

Une caractéristique de la théorie des groupes est qu'il peut y avoir des petits groupes à l'intérieur de groupes plus importants. Le groupe de symétrie du triskèle d'ordre 3 est un sous-groupe du groupe de symétrie du tripode d'ordre 6. J.-L. Lagrange a prouvé un résultat élémentaire sur les sous-groupes. Le théorème de Lagrange énonce que l'ordre d'un sous-groupe doit toujours diviser l'ordre du groupe auquel il appartient. Nous savons donc immédiatement que le groupe de symétrie du tripode n'a aucun sous-groupe d'ordre 4 ou 5.

Classification des groupes Un vaste programme fut lancé pour classer tous les groupes finis possibles. Il n'est pas nécessaire d'en dresser une liste exhaustive car certains groupes sont construits à partir de groupes élémentaires, qui sont les seuls

nécessaires. Le principe de la classification est similaire à ce qui se fait en chimie où l'on ne s'intéresse qu'aux éléments élémentaires et non aux composés qui en dérivent. Le groupe de symétrie du tripode à 6 éléments est un « composé » constitué à partir du groupe des rotations (d'ordre 3) et de celui des réflexions (d'ordre 2).

Presque tous les groupes élémentaires peuvent être classifiés selon des classes connues. Daniel Gorenstein annonça en 1983 que la classification, encore appelée « le théorème énorme », était complète. C'était l'aboutissement de 30 ans d'un travail de recherche qui donna lieu à diverses publications de la part des mathématiciens concernés. C'est un atlas de tous les groupes connus. Les groupes élémentaires appartiennent à quatre types principaux, et malgré tout, on découvrit que 26 groupes n'entrent dans aucune de ces familles. On les appelle les groupes sporadiques.

Les groupes sporadiques sont des groupes marginaux caractérisés par un ordre élevé. Cinq des plus petits étaient connus d'Émile Mathieu dans les années 1860 mais la plupart des découvertes furent faites entre 1965 et 1975. Le groupe sporadique le plus petit est d'ordre 7 920 = $2^4 \times 3^2 \times 5 \times 11$, mais à chaque extrémité de ce groupe, se trouvent le « bébé monstre » et le « monstre ». L'ordre de ce dernier est de $2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$, ce qui, dans le système décimal, est à peu près égal à $8{,}08 \times 10^{53}$ ou, si vous préférez, 8 suivi de 53 zéros. C'est un nombre énorme en effet. On peut montrer que 20 des 26 groupes sporadiques sont des sous-groupes du « monstre », et les six groupes qui échappent à tous les systèmes de classification sont appelés par les Anglo-Saxons les « six parias ».

Les mathématiciens cherchent à formuler les preuves dans un style concis et vigoureux, et pourtant celle de la classification des groupes finis nécessite quelque chose comme 10 000 pages de formules minutieusement argumentées. Les progrès mathématiques ne sont pas toujours le fruit du travail d'un seul génie sublime.

Axiomes pour un groupe

Un ensemble d'éléments G avec une loi notée $\circ$ est un groupe si :
1. Il existe un élément noté 1 de G tel que $1 \circ a = a \circ 1$ pour tous les éléments a du groupe G (1 s'appelle l'élément neutre)

2. Pour chaque élément a de G il existe un élément $\bar{a}$ de G tel que $a \circ \bar{a} = a \circ \bar{a} = 1$ ($\bar{a}$ s'appelle l'élément inverse de a)

3. Pour tous les éléments a, b, et c de G, on a $a \circ (b \circ c) = (a \circ b) \circ c$ (c'est ce que l'on appelle l'associativité).

l'idée clé
Mesure de la symétrie

39 Les matrices

Voici l'histoire de « l'algèbre extraordinaire », révolution mathématique qui s'est produite au milieu du XIXe siècle. Les mathématiciens avaient joué avec des groupes de nombres pendant des siècles, mais l'idée de traiter ces tableaux comme des nombres à part entière a pris son essor il y a 150 ans, grâce à un petit groupe de mathématiciens qui comprirent tout le potentiel de cette idée.

L'algèbre ordinaire n'est autre que cette algèbre traditionnelle dans laquelle des symboles tels que *a, b, c, x* et *y* représentent des nombres à part entière. Cela peut sembler difficile à comprendre, mais pour les mathématiciens, ce fut une avancée fantastique. « L'algèbre extraordinaire » a, quant à elle, entraîné un véritable séisme. S'agissant d'applications sophistiquées, ce passage d'une algèbre de dimension 1 à une algèbre multidimensionnelle a montré la puissance incroyable de son efficacité.

Les nombres à plusieurs dimensions En algèbre ordinaire, a peut représenter un nombre tel que 7, et on écrit alors $a = 7$, mais dans la théorie des matrices une *matrice A* est « un nombre à plusieurs dimensions », comme par exemple le tableau

$$A = \begin{pmatrix} 7 & 5 & 0 & 1 \\ 0 & 4 & 3 & 7 \\ 3 & 2 & 0 & 2 \end{pmatrix}$$

Cette matrice comporte trois lignes et quatre colonnes (c'est une matrice de dimension (3, 4)), mais les matrices peuvent comporter un nombre quelconque de lignes et de colonnes ; on peut même imaginer une matrice géante (100, 200) de 100 lignes et 200 colonnes. Un avantage crucial de l'algèbre des matrices est que l'on peut traiter de vastes regroupements de nombres, des données statistiques par exemple, comme des entités uniques. Plus encore, on peut manipuler ces blocs de nombres de manière simple et efficace. Si l'on veut faire la somme ou le produit de tous les nombres de deux ensembles de données, chacun comportant 1 000 nombres, il n'est pas nécessaire d'effectuer 1 000 calculs. Un seul suffit (qui consiste à faire la somme ou le produit des deux matrices).

chronologie

200 av. J.-C.
Les mathématiciens chinois utilisent des tableaux de nombres.

1850 ap. J.-C.
J. J. Sylvester introduit le terme « matrice ».

1858
Cayley publie *Memoir on the theory of matrices*.

Un exemple concret Supposons que la matrice A représente la production de l'entreprise AJAX en une semaine. L'entreprise AJAX possède trois usines, situées en divers endroits du pays, dont les productions se mesurent en unités (par exemple en milliers d'articles) des quatre produits qu'elle fabrique. Dans notre exemple, les quantités qui correspondent à la matrice A sont :

	produit 1	produit 2	produit 3	produit 4
Usine 1	**7**	**5**	**0**	**1**
Usine 2	**0**	**4**	**3**	**7**
Usine 3	**3**	**2**	**0**	**2**

La semaine suivante, le programme de production peut être différent, mais il peut s'écrire sous la forme d'une nouvelle matrice B. Par exemple, B correspondrait à

$$B = \begin{pmatrix} 9 & 4 & 1 & 0 \\ 0 & 5 & 1 & 8 \\ 4 & 1 & 1 & 0 \end{pmatrix}.$$

Quel est le total de la production pour les deux semaines ? Le théoricien des matrices dit que c'est égal à la somme des matrices $A + B$ où les nombres correspondants sont tous additionnés.

$$A+B = \begin{pmatrix} 7+9 & 5+4 & 0+1 & 1+0 \\ 0+0 & 4+5 & 3+1 & 7+8 \\ 3+4 & 2+1 & 0+1 & 2+0 \end{pmatrix} = \begin{pmatrix} 16 & 9 & 1 & 1 \\ 0 & 9 & 4 & 15 \\ 7 & 3 & 1 & 2 \end{pmatrix}$$

Facile. Malheureusement, la multiplication des matrices est moins évidente. Si l'on retourne à l'entreprise AJAX, on suppose que les profits par unité de ses quatre produits sont de **3**, **9**, **8**, **2**. On peut certainement calculer le bénéfice global pour l'Usine 1 dont les productions des quatre produits sont de 7, 5, 0, 1. Cela donne $7 \times \mathbf{3} + 5 \times \mathbf{9} + 0 \times \mathbf{8} + 1 \times \mathbf{2} = 68$.

Mais plutôt que de ne s'occuper que d'une usine, on peut tout aussi facilement calculer le total T des profits pour toutes les usines :

$$T = \begin{pmatrix} 7 & 5 & 0 & 1 \\ 0 & 4 & 3 & 7 \\ 3 & 2 & 0 & 2 \end{pmatrix} \times \begin{pmatrix} \mathbf{3} \\ \mathbf{9} \\ \mathbf{8} \\ \mathbf{2} \end{pmatrix} = \begin{pmatrix} 7\times\mathbf{3}+5\times\mathbf{9}+0\times\mathbf{8}+1\times\mathbf{2} \\ 0\times\mathbf{3}+4\times\mathbf{9}+3\times\mathbf{8}+7\times\mathbf{2} \\ 3\times\mathbf{3}+2\times\mathbf{9}+0\times\mathbf{8}+2\times\mathbf{2} \end{pmatrix} = \begin{pmatrix} 68 \\ 74 \\ 31 \end{pmatrix}$$

Regardez bien et vous verrez la multiplication de ligne par colonne, caractéristique essentielle du produit des matrices. Si en plus des profits par unité on nous donne

1878
Georg Frobenius prouve certains résultats clés de l'algèbre matricielle.

1925
Heisenberg utilise la mécanique des matrices dans la mécanique quantique.

les volumes par unité **7**, **4**, **1**, **5** de chacune des unités des produits, d'un seul coup, on peut calculer les profits et les besoins en stockage pour les trois usines grâce à une seule multiplication des matrices :

$$\begin{pmatrix} 7 & 5 & 0 & 1 \\ 0 & 4 & 3 & 7 \\ 3 & 2 & 0 & 2 \end{pmatrix} \times \begin{pmatrix} \mathbf{3} & \mathbf{7} \\ \mathbf{9} & \mathbf{4} \\ \mathbf{8} & \mathbf{1} \\ \mathbf{2} & \mathbf{5} \end{pmatrix} = \begin{pmatrix} 68 & 74 \\ 74 & 54 \\ 31 & 39 \end{pmatrix}$$

Le stockage total est fourni par la deuxième colonne de la matrice obtenue, 74, 54 et 39. La théorie des matrices est très puissante. Imaginez la situation d'une entreprise qui a des centaines d'usines, des milliers de produits, des profits par unité et des besoins en stockage différents selon les semaines. Avec l'algèbre des matrices, les calculs, ainsi que notre compréhension, sont pratiquement immédiats et ce, sans avoir à s'inquiéter des détails.

L'algèbre matricielle contre l'algèbre ordinaire On peut établir de nombreux parallèles entre l'algèbre matricielle et l'algèbre ordinaire. La différence la plus connue se trouve au niveau du produit des matrices. Si l'on multiplie la matrice *A* par la matrice *B* puis si on inverse les termes, on obtient :

$$A \times B = \begin{pmatrix} 3 & 5 \\ 2 & 1 \end{pmatrix} \times \begin{pmatrix} 7 & 6 \\ 4 & 8 \end{pmatrix} = \begin{pmatrix} 3\times7+5\times4 & 3\times6+5\times8 \\ 2\times7+1\times4 & 2\times6+1\times8 \end{pmatrix} = \begin{pmatrix} 41 & 58 \\ 18 & 20 \end{pmatrix}$$

$$B \times A = \begin{pmatrix} 7 & 6 \\ 4 & 8 \end{pmatrix} \times \begin{pmatrix} 3 & 5 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 7\times3+6\times2 & 7\times5+6\times1 \\ 4\times3+8\times2 & 4\times5+8\times1 \end{pmatrix} = \begin{pmatrix} 33 & 41 \\ 28 & 28 \end{pmatrix}$$

Dans l'algèbre matricielle, on peut donc avoir $A \times B$ et $B \times A$ qui donnent des résultats différents, situation qui ne se produit pas en algèbre ordinaire où l'ordre des termes de la multiplication n'a pas d'importance.

Une autre différence se produit avec les inverses. En algèbre ordinaire, les inverses sont faciles à calculer. Si $a = 7$ sont inverse est $1/7$ parce que $1/7 \times 7 = 1$. On écrit parfois l'inverse comme suit : $a^{-1} = 7$ et on a donc $a^{-1} \times a = 1$

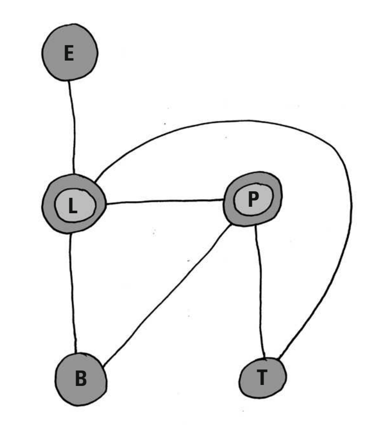
Voici un exemple de la théorie des matrices : $A = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$ et on peut vérifier que

$$A^{-1} = \begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \text{ car } A^{-1} \times A = \begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ où } I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

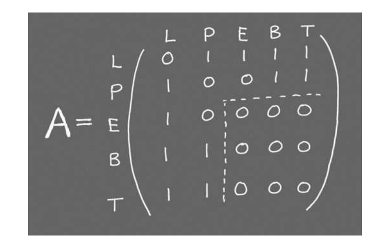
s'appelle la matrice identité et est le pendant de 1 en algèbre ordinaire. En algèbre ordinaire, seul 0 n'a pas d'inverse mais en algèbre matricielle, de nombreuses matrices n'ont pas d'inverse.

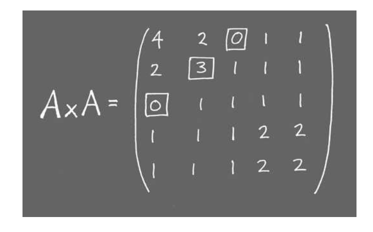
Projets de voyage On trouve un autre exemple de l'utilisation des matrices dans l'analyse des réseaux aériens. Cela concerne à la fois les grandes plaques tournantes du transport aérien et les aéroports plus petits. En pratique, des centaines de destinations peuvent être concernées, et nous allons en voir un exemple : les grands aéroports de **L**ondres (**L**) et **P**aris (**P**), et les aéroports plus petits d'**É**dimbourg (**E**),

Bordeaux (**B**) et **T**oulouse (**T**) et tout le réseau des vols directs possibles. Avant de travailler sur ordinateur pour analyser de tels réseaux, il faut d'abord le programmer en utilisant les matrices. S'il y a un vol direct entre deux aéroports, un 1 est porté à l'intersection de la ligne et de la colonne qui correspondent à ces deux aéroports (comme de **L**ondres à **É**dimbourg). La matrice de « connectivité » qui décrit le réseau ci-dessus s'appelle A.



La sous-matrice inférieure droite d'ordre 3 (délimitée par les pointillés) indique qu'il n'y a pas de vol direct entre les trois aéroports plus petits. Le produit matriciel $A \times A = A^2$ de cette matrice avec elle-même donne le nombre de trajets possibles entre deux aéroports avec une escale unique. Il y a donc par exemple trois allers-retours possibles depuis **P**aris avec escales mais aucun voyage de ce type de **L**ondres à **É**dimbourg. Le nombre de trajets directs ou avec escales est donné par les éléments de la matrice $A + A^2$. C'est un autre exemple de la capacité des matrices à capturer l'essence d'une vaste somme de données au moyen d'un calcul unique.





Lorsqu'un petit groupe de mathématiciens créa la théorie des matrices dans les années 1850, c'était pour résoudre des problèmes de mathématiques pures. D'un point de vue pratique, la théorie des matrices avait tout d'une « solution en quête d'un problème ». Comme cela se produit souvent, des « problèmes » se sont réellement posés qui nécessitaient l'utilisation de la théorie naissante. Une première application eut lieu dans les années 1920 lorsque Werner Heisenberg étudia la « mécanique des matrices », qui est une branche de la mécanique quantique. Autre pionnière dans ce domaine, Olga Taussky-Todd travailla un certain temps dans la conception aéronautique et utilisa l'algèbre des matrices. Quand on lui demanda comment elle avait été amenée à découvrir ce domaine, elle répondit que c'était l'inverse, que c'était la théorie matricielle qui était venue à elle. Tel est le jeu mathématique.

l'idée clé
Combinaisons de tableaux de nombres

40 Les codes

Quel est le point commun entre Jules César et la transmission des signaux numériques modernes ? Réponse courte : les codes et le chiffrement. Pour envoyer des signaux numériques vers un ordinateur ou un téléviseur numérique, il est essentiel de convertir images et discours en une série de zéros et de uns, autrement dit, en un code binaire, car c'est le seul langage que ces appareils comprennent. César se servait de codes pour communiquer avec ses généraux et leur transmettre des messages secrets qu'il rédigeait en substituant chaque lettre par une autre lettre selon une clé que lui seul et ses généraux connaissaient.

La précision était essentielle à César comme elle est aujourd'hui nécessaire pour transmettre efficacement des signaux numériques. César voulait aussi garder pour lui seul le secret de ses codes, et de la même façon, les entreprises de diffusion télévisée du câble et du satellite veulent que leurs seuls abonnés puissent décrypter leurs signaux.

Commençons par la précision. L'erreur humaine ou le « bruit sur la ligne », toujours possibles, doivent être éliminés. La pensée mathématique nous permet de construire des systèmes de codage qui détectent les erreurs automatiquement et qui vont même jusqu'à les corriger.

La détection des erreurs et leur correction L'un des premiers systèmes de code binaire est le Morse qui utilise deux symboles, des points • et des traits –. Son inventeur, Samuel F. B. Morse, envoya le premier message interurbain de Washington à Baltimore avec ce code en 1844. Il l'avait conçu pour le télégraphe électrique du milieu du XIXe siècle sans vraiment se préoccuper de sa fiabilité. Dans le code Morse, la lettre A est représentée par • –, B par – • • •, C par – • – • et les autres lettres par des suites différentes de points et de traits. Pour envoyer le mot « CAB », un opérateur du télégraphe taperait la chaîne – • – • / • – / – • • •. Quels que soient ses mérites, le code Morse n'est pas très habile à détecter les erreurs, alors ne parlons pas de sa capacité à les corriger. Si l'opérateur du code Morse souhaitait envoyer « CAB » mais tapait par erreur un point à la place d'un trait, oubliait le trait dans le A et que du bruit sur la ligne remplaçait un point

chronologie

55 av. J.-C.
Jules César envahit la Bretagne et utilise des codes pour communiquer avec ses généraux.

Vers 1750 ap. J.-C.
le théorème d'Euler pose les fondations du chiffrement à clé publique.

1844
Morse transmet le premier message utilisant le code qui porte son nom.

par un trait, le récepteur qui recevrait • • – • / • / – – • • ne s'apercevrait de rien et traduirait le message par « FEZ ».

On pourrait examiner le système de codage bien plus élémentaire constitué des deux signes 0 et 1 où 0 représente un mot et 1 un autre mot. Supposons qu'un commandant d'armée doive transmettre à ses troupes un message du type « envahissez » ou « n'envahissez pas ». L'instruction « envahissez » est codée par 1 et « n'envahissez pas » par 0. Si un 1 ou un 0 a été retransmis incorrectement, le récepteur ne le saura jamais et transmettra la mauvaise instruction avec les conséquences désastreuses qui s'ensuivront.

On peut améliorer les choses en utilisant des mots de code de longueur 2. Si cette fois on chiffre « envahissez » par 11 et « n'envahissez pas » par 00, une erreur de chiffre donnerait 01 ou 10. Comme seuls 11 ou 00 sont des mots de code légitimes, le récepteur sait avec certitude qu'une erreur s'est produite. L'avantage de ce système est qu'une erreur est décelable, mais on ne sait toujours pas la corriger. Si l'on reçoit 01, comment savoir si c'est 00 ou 11 qui aurait dû être envoyé ?

La solution pour améliorer le système est de construire le message avec des mots de code plus longs. Si l'on chiffre l'instruction « envahissez » par 111 et « n'envahissez pas » par 000, on peut sûrement détecter une erreur dans un chiffre, comme auparavant. Si l'on sait qu'une erreur tout au plus a pu être commise (supposition raisonnable puisque le risque de commettre deux erreurs dans un mot code est faible), le récepteur est en mesure de la corriger. Si l'on reçoit par exemple 110, le message correct est alors 111. Grâce à ces règles, on sait que le message ne peut pas être 000 puisque ce mot de code supposerait deux erreurs. Dans ce système, il y deux mots de code seulement, 000 et 111, mais ils sont suffisamment éloignés pour que soient possibles la détection d'une erreur et sa correction.

Le même principe est utilisé lorsque le traitement de texte est en correction automatique. Si l'on tape « animul », le traitement de texte détecte l'erreur et la corrige en prenant le mot le plus proche, à savoir « animal ». La langue anglaise ne peut cependant pas être totalement soumise à cette correction automatique parce que si l'on tape « lomp » par exemple, plusieurs mots seront voisins : les mots lamp, limp, lump, pomp, et romp ne diffèrent tous de « lomp » que par une seule lettre.

Un code binaire moderne consiste en mots de code constitués d'une série de 0 et de 1. En choisissant des mots de code suffisamment éloignés, la détection et la correction sont toutes deux possibles. Les mots de code du Morse sont trop proches mais les systèmes modernes utilisés pour transmettre des données depuis des satellites peuvent toujours être mis en mode correction automatique. Avec les mots de code

Dans les années 1920
La machine Enigma est mise au point.

1950
Richard Hamming publie un article crucial sur les codes permettant de détecter et corriger les erreurs.

Dans les années 1970
Le chiffrement à clé publique est développé.

longs hautement performants au niveau de la correction d'erreurs, il faut plus de temps pour transmettre les messages et il y a donc une corrélation entre la longueur des mots de code et la vitesse de transmission. Lors des voyages dans l'espace effectués par la NASA, on se sert de codes capables de détecter trois erreurs et suffisamment efficaces pour combattre les bruits parasites.

Coder des messages César se servait de codes pour communiquer avec ses généraux et leur transmettre des messages secrets qu'il rédigeait en substituant chaque lettre par une autre lettre selon une clé que lui seul et ses généraux connaissaient. Si la clé tombait entre de mauvaises mains, ses messages pouvaient être déchiffrés par ses ennemis. À l'époque médiévale, Marie, Reine d'Écosse, envoyait des messages secrets codés depuis sa cellule de prison. Marie avait en tête de renverser sa cousine, la Reine Élizabeth, mais ses messages codés furent interceptés. Plus sophistiqués que le système de codage romain qui consistait à décaler toutes les lettres de l'alphabet d'un certain nombre de positions, ses messages codés reposaient sur des substitutions dont la solution pouvait être découverte par une analyse de la fréquence des lettres et des symboles utilisés. Pendant la Deuxième Guerre Mondiale, le code allemand de la machine Enigma fut déchiffré grâce à la découverte de sa clé. Ce fut extrêmement difficile même si le code restait vulnérable puisque la clé faisait partie du message transmis.

On fit une découverte surprenante en matière de cryptographie dans les années 1970. À l'inverse de tout ce que l'on avait cru jusque-là, on apprenait que la clé secrète pouvait être diffusée à tous et que le message pouvait cependant rester parfaitement sûr. C'est ce que l'on appelle le chiffrement à clé publique. La méthode dépend d'un théorème vieux de 200 ans utilisé dans une branche des mathématiques célébrée pour être la plus utile de toutes.

Le chiffrement à clé publique M. John Sender, agent secret connu dans le milieu des espions sous le pseudonyme « J », vient d'arriver en ville et veut envoyer à son contact le Dr Rodney Receiver un message secret pour annoncer son arrivée. Son comportement est plutôt curieux. Il se rend à la bibliothèque municipale, prend sur une étagère un répertoire de la ville et cherche le nom du Dr R. Receiver. Deux numéros se trouvent à côté du nom Receiver, un long, 247, et un court, 5. Ce renseignement est accessible à n'importe qui, et c'est tout ce dont John Sender a besoin pour coder son message qui est, par souci de simplicité, l'initiale de son prénom. La lettre « J » vient en 74e position dans une liste de mots, qui est elle aussi accessible à tous.

Sender chiffre le numéro 74 en calculant 74^5 modulo 247, autrement dit, il veut connaître le reste de la division de 74^5 par 247. Une simple calculatrice peut le faire, mais il faut travailler avec précision :

$$74^5 = 74 \times 74 \times 74 \times 74 \times 74 = 2\,219\,006\,624$$

et

$$2\,219\,006\,624 = 8\,983\,832 \times 247 + 120$$

La division de ce nombre gigantesque par 247 donne donc un reste de 120. Le message chiffré de Sender est 120, information qu'il transmet à Receiver. Parce que les nombres 247 et 5 sont accessibles à tous, n'importe qui pourrait chiffrer un message. Mais tout le monde ne pourrait le décrypter. Le Dr R. Receiver a certainement quelque chose d'autre en réserve. Il a constitué son numéro personnel 247 en multipliant deux nombres premiers. Dans ce cas, il a obtenu le nombre 247 en multipliant $p = 13$ par $q = 19$, mais il est le seul à le savoir.

C'est là que l'on ressort et dépoussière le vieux théorème que l'on doit à Leonhard Euler. Le Dr R. Receiveur utilise $p = 13$ et $q = 19$ pour trouver une valeur de a telle que

$$a \times 5 \equiv 1 \ (\mathrm{mod}(p-1)(q-1))$$

où le symbole ≡ signifie égal en arithmétique modulaire. Quelle est la valeur de a telle que diviser $5 \times a$ par $12 \times 18 = 216$ donne un reste de 1 ? Il trouve $a = 173$.

Parce qu'il est le seul à connaître les nombres premiers p et q, le Dr Receiver est le seul à pouvoir calculer le nombre 173. Il trouve alors le reste en divisant le gigantesque nombre 120^{173} par 247. Cela dépasse les capacités d'une simple calculatrice mais on peut facilement calculer ce résultat sur un ordinateur. On trouve 74, comme le savait Euler 200 ans auparavant. Muni de ce renseignement, Receiver cherche le mot 74 et voit que « J » est de retour en ville.

Vous allez peut-être dire qu'un pirate informatique pourrait sûrement découvrir que $247 = 13 \times 19$ et que le code serait alors décrypté. Vous auriez raison. Mais les principes de chiffrement et de déchiffrement seraient identiques si le Dr Receiver avait utilisé un autre nombre que 247. Il pourrait choisir deux très gros nombres premiers et en faire le produit pour obtenir un nombre supérieur à 247.

Trouver les deux facteurs premiers d'un très grand nombre est virtuellement impossible – quels sont les facteurs de 24 812 789 922 307 par exemple ? Mais on pourrait aussi choisir des nombres bien supérieurs à celui-là. Le chiffrement à clé publique est fiable et si la puissance de plusieurs super-ordinateurs réunie permet de décomposer une clé de chiffrement en produits de deux facteurs premiers, il suffit au Dr Receiver de prendre un nombre supérieur encore. Pour finir, il est considérablement plus facile pour le Dr Receiver de « mélanger des boîtes de sable noir et de sable blanc » que pour un pirate informatique de trier les grains de sable.

l'idée clé
Garder des messages secrets

41 Le dénombrement

La branche des mathématiques appelée analyse combinatoire est parfois connue sous le nom de dénombrement. Il ne s'agit pourtant pas ici d'additionner de tête une colonne de chiffres. « Combien » est un problème, mais « Comment les objets peuvent-ils être dénombrés » en est un également. Les problèmes de ce type sont souvent formulés avec simplicité et ne s'encombrent pas de la lourde superstructure de la théorie mathématique ; vous n'avez nul besoin d'avoir de larges prérequis pour vous retrousser les manches. C'est ce qui plaît dans les problèmes combinatoires. Mais il faudrait signaler qu'ils comportent des risques pour la santé : un effet d'accoutumance est possible et ils sont très souvent à l'origine d'insomnies.

Un conte de Saint Ives Les enfants peuvent commencer l'analyse combinatoire dès leur plus jeune âge. Une comptine anglaise traditionnelle pose un problème de dénombrement :

En route pour Saint Ives,
Je rencontrai un homme qui avait sept femmes ;
Chaque femme portait sept sacs,
Chaque sac contenait sept chats,
Chaque chat avait sept chatons.
Chatons, chats, sacs et femmes,
Combien étaient-ils en route pour Saint Ives ?

Le dernier vers pose un problème délicat (réponse : au moins une personne). Mais on peut toujours formuler un problème différemment : combien étaient-ils à venir de Saint Ives ?

L'interprétation que l'on fait du texte est importante. Peut-on être sûr que l'homme et ses sept femmes revenaient tous de Saint Ives ? Les femmes accompagnaient-elles l'homme lorsque je l'ai rencontré, ou se trouvaient-elles ailleurs ? Un problème d'analyse combinatoire doit d'abord être énoncé clairement pour être parfaitement compris.

On suppose que les compagnons de l'homme revenaient tous de la ville côtière de Cornouailles par le même chemin, et que les « chatons, chats, sacs et femmes »

chronologie

Vers 1800 av. J.-C.
Le papyrus Rhind est rédigé en Égypte.

Vers 1100 ap. J.-C.
Bhaskara étudie les permutations et les combinaisons.

étaient tous présents. Combien venaient de Saint Ives ? Le tableau suivant nous donne une réponse.

Homme	1	1
Femmes	7	7
Sacs	7×7	49
Chats	$7 \times 7 \times 7$	343
Chatons	$7 \times 7 \times 7 \times 7$	2 401
Total		**2 801**

Lors d'un séjour à Luxor en 1858, Alexander Rhind, antiquaire écossais, découvrit par hasard un papyrus de 5 mètres de long couvert de formules mathématiques remontant à 1800 av. J.-C. Il l'acheta. Quelques années plus tard, le British Museum l'acquit et les hiéroglyphes furent traduits. Le problème 79 du Papyrus Rhind est un problème de maisons, de chats, de souris et de blé qui ressemble fortement à celui des chatons, chats, sacs et femmes de Saint Ives. Ils impliquent tous deux des puissances de 7 et le même type d'analyse. L'analyse combinatoire a, semble-t-il, une bien longue histoire.

Les factorielles Avec le problème des files d'attente, nous sommes en présence de la première arme de l'arsenal combinatoire : les *factorielles*. Supposons qu'Alban, Brice, Charlotte, David et Émilie forment une file d'attente

E C A B D.

Émilie est en tête, suivie de **C**harlotte, d'**A**lban et de **B**rice qui est lui-même suivi de **D**avid, le dernier de la file. Si l'on change les personnes de place, on obtient d'autres files d'attente ; combien de files d'attente différentes sont-elles possibles ?

L'art du dénombrement dans ce problème dépend du *choix*. Il existe 5 choix possibles pour la personne qui occupera la première place de la file, et une fois que cette personne a été choisie, il existe 4 choix pour la seconde, et ainsi de suite. Lorsque l'on arrive à la dernière position, il ne reste aucun choix possible car elle ne peut être occupée que par la dernière personne non placée. Il y a donc $5 \times 4 \times 3 \times 2 \times 1 = 120$ files d'attente possibles. Si l'on avait commencé avec 6 personnes, le nombre de files possibles serait $6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720$ et pour 7 personnes, il y aurait $7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5\,040$ files possibles.

Le produit de nombres entiers consécutifs de 1 à n s'appelle une factorielle. On en trouve si souvent en mathématiques que l'on préfère les écrire sous la forme 5! (qui se lit « factorielle 5 ») plutôt que sous la forme $5 \times 4 \times 3 \times 2 \times 1$. Examinons les

1850
Kirkman pose le problème des 15 pensionnaires.

1930
Franck Ramsey travaille dans le domaine de l'analyse combinatoire.

1971
Ray-Chaudhuri et Wilson prouvent l'existence des systèmes généraux de Kirkman.

premières factorielles (par convention, on définit 0! = 1). On se rend immédiatement compte que de « petites » configurations génèrent de « grandes » factorielles. Peu importe si le nombre n est petit, n! peut être énorme.

nombre	factorielle
0	1
1	1
2	2
3	6
4	24
5	120
6	720
7	5 040
8	40 320
9	362 880

Si l'on cherche toujours à former des files d'attente de 5 personnes, mais que nous pouvons à présent les prendre dans un ensemble de 8 personnes **A**, **B**, **C**, **D**, **E**, **F**, **G** et **H**, l'analyse est pratiquement la même. Il y a 8 choix pour la première personne de la file, 7 pour la seconde, et ainsi de suite. Mais cette fois, il existe 4 choix possibles pour occuper la dernière place. Le nombre de files possibles est égal à

$$8 \times 7 \times 6 \times 5 \times 4 = 6\,720.$$

On peut écrire ce résultat avec des factorielles parce que

$$8 \times 7 \times 6 \times 5 \times 4 = 8 \times 7 \times 6 \times 5 \times 4 \times \frac{3 \times 2 \times 1}{3 \times 2 \times 1} = \frac{8!}{3!}$$

Les combinaisons Dans une file, *l'ordre* est important.

Les deux files

C E B A D D A C E B

contiennent les mêmes lettres mais constituent des files différentes. On sait déjà que l'on peut former 5! files à partir de ces lettres. Si l'on veut trouver le nombre de façons différentes de sélectionner 5 personnes parmi 8 sans tenir compte de l'ordre, il faut diviser 8 × 7 × 6 × 5 × 4 = 6 720 par 5!. Le nombre de façons de sélectionner 5 personnes parmi 8 est donc égal à

$$\frac{8 \times 7 \times 6 \times 5 \times 4}{5 \times 4 \times 3 \times 2 \times 1} = 56.$$

Ce nombre s'écrit $\binom{8}{5}$ (ou C_5^8), qui est égal à

$$\binom{8}{5} = \frac{8!}{3!\,5!} = 56.$$

Au loto, il faut choisir 6 nombres parmi 49 possibles ; combien y a-t-il donc de possibilités ?

$$\binom{49}{6} = \frac{49!}{43!\,6!} = \frac{49 \times 48 \times 47 \times 46 \times 45 \times 44}{6 \times 5 \times 4 \times 3 \times 2 \times 1} = 13\,983\,816.$$

Une seule combinaison est gagnante. Il y a donc environ 1 chance sur 14 millions de gagner le gros lot.

Le problème de Kirkman L'analyse combinatoire est un vaste domaine connu depuis des siècles, mais qui ne s'est développé que ces 40 dernières années grâce à l'informatique. On peut considérer que les problèmes de théorie des graphes, des carrés latins et des autres du même genre font partie de l'analyse combinatoire moderne.

Le principe de l'analyse combinatoire est bien mis en évidence par un maître en la matière, le Révérend Thomas Kirkman, dans la deuxième moitié du XIXe siècle, alors qu'elle était surtout liée aux mathématiques récréatives. Ses contributions nombreuses et originales à la géométrie discrète, à la théorie des groupes et à l'analyse combinatoire ne lui permirent cependant pas d'obtenir un poste à l'université. Le casse-tête qui consolida sa réputation de mathématicien du non-sens est celui qui lui valut la célébrité. En 1850, Kirkman présenta le « problème des 15 pensionnaires ». De jeunes pensionnaires se rendent à l'église en formant 5 rangs de 3 jeunes filles chaque jour de la semaine. Si vous êtes fatigué des Sudoku, essayez ce problème. Il faut établir un planning journalier pour éviter que deux élèves ne soient ensemble plus d'une fois par semaine. Utilisant minuscules et majuscules à dessein, les prénoms des jeunes filles sont les suivants : **a**rmelle, **b**éatrice, **c**lémence, **d**orothée, **e**mma, **f**rancine, **g**râce, **A**gnès, **B**érénice, **C**harlotte, **D**anielle, **E**dith, **F**lorence, **G**aëlle et **V**ictoire. On les désigne respectivement par **a**, **b**, **c**, **d**, **e**, **f**, **g**, **A**, **B**, **C**, **D**, **E**, **F**, **G** et **V**.

Il existe en réalité sept solutions différentes au problème de Kirkman, et celle que nous donnerons est dite « cyclique » : elle est générée par « permutation » des jeunes filles. C'est là que se justifie le choix de les désigner par des minuscules et des majuscules.

Lundi			Mardi			Mercredi			Jeudi			Vendredi			Samedi			Dimanche		
a	**A**	**V**	**b**	**B**	**V**	**c**	**C**	**V**	**d**	**D**	**V**	**e**	**E**	**V**	**f**	**F**	**V**	**g**	**G**	**V**
b	**E**	**D**	**c**	**F**	**E**	**d**	**G**	**F**	**e**	**A**	**G**	**f**	**B**	**A**	**g**	**C**	**B**	**a**	**D**	**C**
c	**B**	**G**	**d**	**C**	**A**	**e**	**D**	**B**	**f**	**E**	**C**	**g**	**F**	**D**	**a**	**G**	**E**	**b**	**A**	**F**
d	**f**	**g**	**e**	**g**	**a**	**f**	**a**	**b**	**g**	**b**	**c**	**a**	**c**	**d**	**b**	**d**	**e**	**c**	**e**	**f**
e	**F**	**C**	**f**	**G**	**D**	**g**	**A**	**E**	**a**	**B**	**F**	**b**	**C**	**G**	**c**	**D**	**A**	**d**	**E**	**B**

La solution est cyclique car chaque jour, le calendrier des promenades est modifié comme suit : **a** est remplacée par **b**, **b** par **c**, et ainsi de suite jusqu'à **g** remplacée par **a**. De même pour les pensionnaires désignées par des majuscules : **A** est remplacée par **B**, **B** est remplacée par **C** et ainsi de suite, mais **V**ictoire n'est jamais remplacée.

La raison cachée du choix de cette notation est que les rangs correspondent aux lignes dans le plan de Fano (voir p. 115). Le problème de Kirkman n'est pas un simple divertissement ; il figure parmi les grands problèmes mathématiques classiques.

l'idée clé
Combien de combinaisons ?

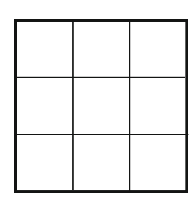
42 Les carrés magiques

« Le mathématicien », écrivait G. H. Hardy, « à l'instar du peintre ou du poète, crée des formes ». Les carrés magiques présentent des formes très curieuses, même d'un point de vue mathématique. Elles se situent quelque part entre ces formules mathématiques chargées de symboles et ces figures fascinantes dont raffolent les créateurs de casse-tête.

Un carré magique est une grille carrée divisée en cases, où sont disposés des entiers distincts de manière à ce que la somme sur chaque ligne horizontale, verticale (ou colonne) mais aussi sur chaque diagonale soit identique.

a	*b*
c	*d*

Les carrés constitués d'une seule ligne et d'une seule colonne sont, techniquement parlant, des carrés magiques, mais ils présentent trop peu d'intérêt pour que l'on s'y attarde. Il n'existe pas de carré magique constitué de deux lignes et deux colonnes. Si un tel carré existait, il prendrait la forme ci-contre. Comme la somme des lignes et la somme des colonnes seraient égales, alors $a + b = a + c$. Autrement dit, $b = c$, ce qui va à l'encontre de l'obligation pour les entrées d'être toutes distinctes.



Le carré Lo Shu Des carrés magiques de 2×2 cases (ou d'ordre 2) n'existent pas, c'est pourquoi nous examinerons des carrés 3×3 pour lesquels nous établirons des grilles. Nous commencerons avec un carré magique *normal*, c'est-à-dire un carré dont les cases sont remplies avec les chiffres consécutifs 1, 2, 3, 4, 5, 6, 7, 8 et 9.

Avec un carré si petit, on peut construire un carré magique d'ordre 3×3 par tâtonnement, mais on peut d'abord procéder par déductions. Si l'on fait la somme de tous les nombres de la grille, on obtient

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45$$

et ce résultat doit être égal à la somme des 3 lignes. Cela montre que la somme de chaque ligne (ainsi que la somme de chaque colonne et diagonale) est égale à 15.

chronologie

Vers 2800 av. J.-C.
La légende du carré de Lo Shu voit le jour.

Vers 1690 ap. J.-C.
De La Loubère produit la méthode siamoise de construction des carrés magiques.

Examinons maintenant la case du milieu, que nous appellerons *c*. Deux diagonales contiennent *c*, de même que la ligne du milieu et la colonne du milieu. Si l'on fait la somme totale de ces quatre lignes, on obtient 15 + 15 + 15 + 15 = 60 et cette somme doit être égale à la somme de tous les nombres à laquelle s'ajoute $3c$. L'équation $3c + 45 = 60$ ainsi obtenue nous permet de déduire que *c* doit être égal à 5. On apprend aussi qu'il est impossible de placer le chiffre 1 dans une case de coin. Après avoir réuni quelques indices, nous sommes en mesure d'utiliser la méthode par tâtonnement. Allez-y, essayez !

8	1	6
3	5	7
4	9	2

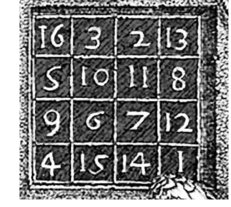
Une solution pour le carré d'ordre 3 par la méthode siamoise

Bien sûr, on aimerait disposer d'une méthode totalement rigoureuse pour construire des carrés magiques. Simon de La Loubère, ambassadeur français du roi de Siam à la fin du XVIIe siècle, en trouva une. La Loubère s'intéressait aux mathématiques chinoises et rédigea une méthode pour construire des carrés magiques constitués d'un nombre impair de lignes et de colonnes. On commence en plaçant le chiffre 1 au milieu de la ligne inférieure, puis l'on suit « la diagonale et on revient de l'autre côté de la grille si nécessaire » pour noter le 2 et les nombres qui suivent. Si la case est occupée, on place le nombre suivant au-dessus de la dernière case remplie.

Fait notable, ce carré magique normal est absolument le seul à être constitué de 3 lignes et 3 colonnes. Tous les autres carrés magiques 3 × 3 peuvent s'obtenir à partir de celui-ci par une rotation des nombres par rapport au milieu et/ou par symétrie des nombres par rapport à la colonne du milieu ou de la ligne du milieu. Ce carré appelé carré « Lo Shu » était connu en Chine vers 3000 av. J.-C. La légende dit qu'il a d'abord été repéré sur la carapace d'une tortue qui sortait du fleuve Lo. Les habitants du lieu y virent un signe des dieux qui leur signifiaient que la peste continuerait à sévir s'ils ne faisaient pas davantage d'offrandes.

S'il existe un seul carré magique 3 × 3, combien de carrés magiques d'ordre 4 existe-t-il ? La réponse va vous stupéfier : il en existe 880 différents (et accrochez-vous, il y en a 2 202 441 792 d'ordre 5). On ne sait pas combien il existe de carrés pour des valeurs générales de *n*.

Les carrés de Dürer et de Franklin Le carré magique Lo Shu est réputé pour être à la fois unique et chargé d'histoire, mais il existe un carré magique d'ordre 4 × 4 qui est devenu une véritable icône en raison de son lien avec un artiste célèbre. Ce carré est également pourvu d'un bien plus grand nombre de propriétés que certains des 880 carrés magiques 4 × 4 ordinaires. Il s'agit du carré 4 × 4 représenté en 1514 sur la gravure *Melancholia* d'Albrecht Dürer.



Dans ce carré de Dürer, la somme de toutes les lignes est égale à 34, et il en va de même pour la somme des colonnes, diagonales, et petits carrés

1693
Bernard Frénicle de Bessy dresse la liste des 880 carrés magiques possibles d'ordre 4.

1770
Euler produit un carré de carrés parfaits.

1986
Sallows crée un carré à partir de lettres.

52	61	4	13	20	19	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

d'ordre 2 qui constituent le carré complet 4 × 4. Dürer a même réussi à signer son chef-d'œuvre en notant la date de l'achèvement de son œuvre au milieu de la ligne inférieure.

Le scientifique et diplomate américain Benjamin Franklin comprit que construire des carrés magiques était un moyen utile de s'aiguiser l'esprit. C'était un expert en la matière, et aujourd'hui encore, les mathématiciens ne savent pas très bien comment il s'y prenait ; les grands carrés magiques ne peuvent pas être le fruit d'une heureuse coïncidence. Franklin confessa que, dans sa jeunesse, il avait consacré beaucoup de temps à cette activité malgré son peu d'attirance pour « l'Arithmétik » à l'école. Voici une de ses créations de jeunesse.

Dans ce carré magique normal, il y a toutes sortes de symétries. La somme de toutes les lignes, colonnes et diagonales est égale à 260, de même que celle des « arcs », dont un exemple a été grisé sur le dessin. Beaucoup d'autres choses restent à découvrir, comme le fait que la somme du carré central 2 × 2 ajoutée à la somme des cases des quatre coins est aussi égale à 260. Regardez bien, et vous trouverez un résultat intéressant pour chaque carré 2 × 2.

127^2	46^2	58^2
2^2	113^2	94^2
74^2	82^2	97^2

Carrés de carrés Les cases de certains carrés magiques peuvent être occupées par des carrés parfaits. Le problème que pose leur construction a été présenté par le mathématicien français Edouard Lucas en 1876. À ce jour, aucun carré 3 × 3 constitué de carrés parfaits n'a pu être trouvé, même s'il s'en est fallu de peu.

Toutes les lignes, colonnes ainsi qu'une diagonale de ce carré ont pour somme magique 21 609 mais l'autre diagonale ne donne pas ce résultat puisque $127^2 + 113^2 + 97^2 = 38\,307$. Si vous avez envie de trouver un tel carré par vous-même, vous devriez noter ce résultat prouvé : la valeur de la case centrale doit être supérieure à $2{,}5 \times 10^{25}$ et il ne sert donc à rien de chercher à construire un carré avec de petits nombres ! Ce sont là des mathématiques solides qui ont un lien avec les courbes elliptiques, outils qui permettent de démontrer le grand théorème de Fermat. On a prouvé qu'il n'existe aucun carré magique 3 × 3 dont les entrées sont des cubes ou des puissances quatrièmes.

La recherche de carrés de carrés parfaits s'est malgré tout révélée fructueuse pour des carrés plus grands. Des carrés magiques 4 × 4 et 5 × 5 constitués de carrés parfaits existent bel et bien. En 1770, Euler en produisit un exemple sans expliquer sa méthode de construction. Des familles complètes de ces carrés furent découvertes depuis lors qui ont un lien avec l'étude de l'algèbre des quaternions, nombres imaginaires à quatre dimensions.

Les carrés magiques exotiques Il se peut que les grands carrés magiques aient des propriétés spectaculaires. Une grille de 32 × 32 a été produite par l'expert

en carrés magiques William Benson. C'est un carré magique qui reste magique si l'on élève les nombres qu'il contient au carré ou au cube. En 2001, un carré magique d'ordre 1 024 a été créé, carré qui est également magique si l'on élève chacun de ses éléments aux puissances 2, 3, 4 et 5. Il existe de nombreux exemples de ce type.

On peut créer une variété entière d'autres carrés magiques si l'on allège les conditions. Les carrés magiques normaux sont courants. Si l'on retire la condition selon laquelle la somme des éléments des diagonales doit être égale à chacune des sommes des lignes et des colonnes, il s'ensuit alors une pléthore de résultats spécifiques. On peut chercher des carrés dont les éléments ne sont que des nombres premiers, ou on peut considérer d'autres formes que des carrés elles aussi dotées de « propriétés magiques ». L'étude de dimensions supérieures nous amène à étudier les cubes et les hypercubes magiques.

Le prix du carré magique le plus extraordinaire, parce qu'il est vraiment curieux, revient à un modeste carré d'ordre 3 créé par le hollandais Lee Sallows, ingénieur en électronique et spécialiste des jeux de mots :

5	22	18
28	15	2
12	8	25

Qu'y a-t-il là de si remarquable ? Écrivez d'abord ces nombres en toutes lettres et en anglais :

five	twenty-two	eighteen
twenty-eight	fifteen	two
twelve	eight	twenty-five

Comptez ensuite le nombre de lettres qui constituent chaque mot :

4	9	8
11	7	3
6	5	10

Ce qui est remarquable, c'est qu'il s'agit d'un carré magique constitué des nombres consécutifs 3, 4, 5 jusqu'à 11. De plus, le nombre de lettres des sommes magiques des deux carrés d'ordre 3 (21 ou « twenty-one » et 45 ou « forty-five ») est égal à 9, et 3 × 3 = 9.

l'idée clé
Sorcellerie mathématique

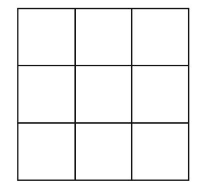
43 Les carrés latins

Depuis quelques années, la folie du Sudoku a gagné le monde entier. Partout, on mâchonne crayons et stylos dans l'attente de la bonne inspiration qui donnera le chiffre à écrire dans la case. Est-ce 4 ou est-ce 5 ? Peut-être est-ce 9. Lorsque les voyageurs émergent de leur train le matin, ils ont déjà fourni plus d'effort mental qu'ils n'en fourniront le reste de la journée. Le soir, le dîner brûle dans le four. Est-ce 5, 4 ou peut-être 7 ? En jouant, tous ces gens se révèlent mathématiciens.

	4		8		3			
		7						3
		9	7			2	6	
3				1		7		9
			6	9	8			
1		5		2				6
	2	3			6	5		
6						1		
			5		2		8	

Résolution du Sudoku Dans le jeu du Sudoku, on a une grille 9 × 9 qui contient quelques chiffres. Le but est de remplir le reste des cases en utilisant les chiffres donnés comme indices. Chaque ligne et chaque colonne doivent contenir chacun des chiffres 1, 2, 3, …, 9 une seule fois et il en va de même pour chacun des carrés 3 × 3 que comporte la grille.

On pense que le Sudoku (qui signifie « chiffres uniques ») a été inventé à la fin des années 1970. Il s'est d'abord répandu au Japon dans les années 1980 avant de gagner le monde à partir de 2005. L'attrait de ce casse-tête est que, contrairement aux mots croisés, il ne nécessite pas une vaste culture, mais, comme les mots croisés, c'est un jeu très prenant. Les passionnés qui s'infligent ces deux formes de torture ont de nombreux points communs.



Les carrés latins 3 × 3 Un tableau carré qui contient exactement un symbole unique dans chaque ligne et chaque colonne s'appelle un carré latin. Le nombre de symboles est égal à la taille du carré et s'appelle son « ordre ». Peut-on remplir une grille vide 3 × 3 de sorte que chaque ligne et chaque colonne contiennent exactement l'un des symboles *a*, *b*, et *c* ? Si oui, alors on aurait un carré latin d'ordre 3.

Lorsqu'il introduisit le concept de carré latin, Leonhard Euler parla d'une nouvelle sorte de carré magique. Contrairement aux carrés magiques, cependant, les carrés latins n'ont rien à voir avec l'arithmétique et il n'est pas nécessaire de prendre des

chronologie

1779
Euler explore la théorie des carrés latins.

1900
Tarry montre qu'il n'existe pas de carrés latins orthogonaux d'ordre 6.

nombres pour symboles. On les appelle ainsi tout simplement parce que les symboles utilisés pour les remplir viennent de l'alphabet latin, alors qu'Euler utilisait le grec dans les autres carrés.

Un carré latin 3 × 3 est facile à trouver.

a	*b*	*c*
b	*c*	*a*
c	*a*	*b*

Si l'on considère que les lettres *a*, *b*, et *c* désignent le lundi, le mardi et le vendredi, on pourrait utiliser le carré pour programmer des rencontres entre deux équipes. L'équipe Une est constituée de **L**ucie, **M**arie et **N**ancy et l'équipe Deux de **R**omain, **S**ophie et **T**homas.

	R	**S**	**T**
L	*a*	*b*	*c*
M	*b*	*c*	*a*
N	*c*	*a*	*b*

Marie, de l'équipe Une, a par exemple une rencontre avec **T**homas de l'équipe Deux le lundi (l'intersection de la ligne **M** avec la colonne **T** est *a* = Lundi). L'arrangement du carré latin garantit qu'une rencontre a lieu entre chaque paire de membres des équipes et que les dates ne se chevauchent pas.

Ce n'est pas le seul carré latin 3 × 3 possible. Si l'on interprète *A*, *B*, et *C* comme des sujets abordés lors de rencontres entre l'équipe Une et l'équipe Deux, on peut produire un carré latin qui garantit que chaque personne aborde un sujet différent avec un membre de l'autre équipe.

	R	**S**	**T**
L	*A*	*B*	*C*
M	*C*	*A*	*B*
N	*B*	*C*	*A*

Marie, de l'équipe Une, aborde donc le sujet *C* avec **R**omain, le sujet *A* avec **S**ophie et le sujet *B* avec **T**homas.

Quel jour chacune des discussions devrait-elle avoir lieu, entre qui et qui, et sur quel sujet ? Quel serait le programme de cette organisation complexe ? Par chance, les deux carrés latins peuvent être combinés symbole par symbole pour produire un carré latin composé, dans lequel chacune des neuf paires qui associent un jour et un sujet possibles ne se produisent qu'une seule fois.

	R	**S**	**T**
L	*a,A*	*b,B*	*c,C*
M	*b,C*	*c,A*	*a,B*
N	*c,B*	*a,C*	*b,A*

1925
Fisher suggère d'utiliser les carrés latins pour concevoir des expériences statistiques.

1960
La conjecture d'Euler sur la non-existence de certaines paires de carrés latins est infirmée par Bose, Parker et Shrikhande.

1979
Des jeux du type du Sudoku sont inventés à New York.

On trouve une autre interprétation du carré dans le « problème des neuf officiers », problème historique dans lequel neuf officiers appartenant à trois régiments *a*, *b* et *c* et de grades différents *A*, *B* et *C* sont placés sur un terrain de manœuvres de sorte que chaque ligne et chaque colonne contiennent un officier de chaque régiment et de grade différent. Les carrés latins de ce type sont dits « orthogonaux ». Le cas du carré 3×3 est simple mais trouver des paires de carrés latins orthogonaux pour construire de plus grands carrés est loin d'être facile. Il fallait tout le génie d'Euler pour y parvenir.

Dans le cas du carré latin 4×4, un « problème de 16 officiers » consisterait à arranger les 16 figures d'un jeu de cartes dans un carré de sorte qu'il y ait une valeur (As, Roi, Dame, ou Valet) et une couleur (pique, trèfle, cœur, ou carreau) dans chaque ligne et dans chaque colonne. En 1782, Euler a posé le même problème pour « 36 officiers ». Cela revenait à rechercher deux carrés orthogonaux d'ordre 6. Il ne parvint pas à les trouver et conjectura qu'il n'existait aucune paire de carrés latins orthogonaux d'ordre 6, 10, 14, 18, 22, … Peut-on le prouver ?

Vint ensuite Gaston Tarry, mathématicien amateur qui était fonctionnaire en Algérie. Il examina soigneusement quelques exemples et en 1900 avait vérifié la conjecture d'Euler pour un cas : il n'existe pas de paire de carrés latins orthogonaux d'ordre 6. Les mathématiciens pensèrent tout naturellement qu'Euler avait raison pour les autres cas d'ordre 10, 14, 18, 22, …

En 1960, les efforts combinés de trois mathématiciens stupéfièrent le monde mathématique en prouvant qu'Euler s'était trompé pour tous les autres cas. Raj Bose, Ernest Parker et Sharadchandra Shrikhande prouvèrent qu'il y avait bien des paires de carrés latins orthogonaux d'ordre 10, 14, 18, 22, … Le seul et unique cas où les carrés latins n'existent pas (mis à part les carrés sans intérêt d'ordre 1 et 2) est celui d'ordre 6.

Nous avons vu qu'il existe deux carrés latins d'ordre 3 mutuellement orthogonaux. Pour l'ordre 4, on peut produire trois carrés mutuellement orthogonaux. On peut montrer qu'il n'y a jamais plus de $n - 1$ carrés latins mutuellement orthogonaux d'ordre n, et donc pour $n = 10$, par exemple, il ne peut y avoir plus de neuf carrés mutuellement orthogonaux mais les trouver est une autre paire de manches. À ce jour, personne n'a réussi à produire ne serait-ce que trois carrés latins mutuellement orthogonaux d'ordre 10.

À quoi servent les carrés latins ? R. A. Fisher, éminent statisticien, comprit que les carrés latins avaient un intérêt pratique. Il s'en servit pour révolutionner les méthodes agricoles de son époque au centre de recherche de Rothamsted situé dans le Hertfordshire, au Royaume-Uni.

Le but de Fisher était d'étudier l'efficacité des engrais sur les productions. Dans l'idéal, on aimerait que les cultures soient plantées dans des sols identiques de sorte que la qualité du sol ne soit pas un facteur indésirable qui pourrait modifier la production. On pourrait donc appliquer les différents engrais en toute tranquillité

puisque le « problème » de la qualité du sol serait éliminé. La seule manière de garantir des conditions de sols identiques serait d'utiliser le même sol, mais d'un point de vue pratique, on ne peut pas s'amuser à arracher puis replanter la production. Même si on le pouvait, des conditions météo différentes poseraient un autre problème.

Une solution possible est d'utiliser les carrés latins. Examinons le cas où il s'agit de tester quatre produits. Si l'on divise un champ carré en 16 lots, on peut imaginer que le carré latin nous donne une description « verticale » et « horizontale » de la qualité du sol.

Les quatre engrais sont ensuite appliqués aléatoirement sur les lots *a*, *b*, *c* et *d*, de sorte qu'un seul produit soit appliqué dans chaque ligne et dans chaque colonne pour éliminer le problème de la variation de la qualité du sol. Si l'on soupçonne l'existence d'un autre facteur qui pourrait modifier la production, on pourrait aussi régler ce problème. Supposons que nous estimions que le moment de la journée où nous appliquons le traitement est un facteur indésirable. Appelons les zones horaires de la journée *A*, *B*, *C* et *D* et utilisons les carrés latins orthogonaux pour réunir les données. On a ainsi l'assurance que chaque traitement et chaque zone horaire apparaît dans un lot. L'expérience pourrait alors être menée comme suit :

a, temps *A*	*b*, temps *B*	*c*, temps *C*	*d*, temps *D*
b, temps *C*	*a*, temps *D*	*d*, temps *A*	*c*, temps *B*
c, temps *D*	*d*, temps *C*	*a*, temps *B*	*b*, temps *A*
d, temps *B*	*c*, temps *A*	*b*, temps *D*	*a*, temps *C*

D'autres facteurs peuvent être passés au crible en continuant à créer des versions encore plus élaborées de carrés latins. Euler n'aurait pas pu imaginer que la solution de son problème d'officiers serait appliquée à des expériences agricoles.

l'idée clé
Le mystère du Sudoku mis au jour

44 Les mathématiques financières

Norman est un super vendeur de bicyclettes. Il considère qu'il est de son devoir de mettre tout le monde sur un vélo, et il est ravi lorsqu'un client se présente dans son magasin et lui en achète un sans hésiter pour 99 €. Le client paie avec un chèque de 150 €, et comme les banques sont fermées, Norman demande à son voisin de lui faire la monnaie de ce chèque. Il revient, rend 51 € à son client qui s'en va alors à toute vitesse sur son vélo. Et c'est le désastre. Le chèque est sans provision, le voisin demande qu'on lui rende son argent, et Norman doit aller emprunter cet argent auprès d'un ami. Le vélo lui a coûté 79 € au départ, mais combien Norman a-t-il perdu au total ?

Le concept de cette petite énigme fut proposé par le grand créateur de casse-tête Henry Dudeney. Il s'agit là, si l'on peut dire, de mathématiques financières, ou, pour être plus précis, d'un casse-tête où il est question d'argent. Il montre comment l'argent est assujetti au temps mais aussi que l'inflation a de beaux jours devant elle. À l'époque où Dudeney écrivait, dans les années 1920, le dit vélo coûtait sept fois moins cher au client. Il est possible de combattre l'inflation grâce aux intérêts. Ce sont des trucs que l'on trouve dans les mathématiques les plus sérieuses ainsi que sur les marchés financiers modernes.

Intérêts composés Il existe deux sortes d'intérêts connus sous le nom d'intérêts simples ou composés. Tournons nos projecteurs mathématiques vers deux frères, Charles et Simon. Leur père leur donne à chacun 1 000 €, qu'ils placent tous deux à la banque. Charles choisit toujours des placements à intérêts composés tandis que Simon, plus traditionnel, préfère les placements à intérêts simples. Historiquement, les intérêts composés étaient assimilés à l'usure, pratique que l'on décriait alors. De nos jours, les intérêts composés sont incontournables, en particulier dans les systèmes monétaires modernes. Les intérêts composés sont des intérêts générés par les intérêts eux-mêmes, et c'est ce qui plaît à Charles. Les intérêts simples n'ont pas cette caractéristique et sont calculés à partir d'une somme initiale

chronologie

3000 av. J.-C.
Les Babyloniens utilisent un système en base 60 pour les opérations financières.

1494
Luca Pacioli publie des tables financières et un relevé de comptabilité en partie double.

appelée « un principal » ou « un capital ». Pour Simon, c'est plus facile à comprendre puisque le capital génère les mêmes intérêts chaque année.

Lorsque l'on parle mathématiques, il est toujours intéressant d'avoir Albert Einstein à portée de main, mais contrairement à cette idée largement répandue, il n'a sûrement jamais dit que les intérêts composés étaient la plus grande découverte de tous les temps. Que la formule des intérêts composés nous concerne de manière plus immédiate que la formule $E = mc^2$ est indéniable. Si vous économisez ou empruntez de l'argent, utilisez une carte de crédit, obtenez un prêt pour un logement ou achetez un viager, la formule de l'intérêt composé travaille discrètement pour (ou contre) vous. Que représentent les symboles ? Le terme P désigne le principal (l'argent que vous économisez ou empruntez), i est le taux d'intérêt exprimé en pourcentage et n correspond au nombre de périodes.

$$A = P \times (1 + i)^n$$

Formule des intérêts composés

Charles place ses 1 000 € sur un compte qui lui rapporte 7 % d'intérêts annuels. De combien ce capital va-t-il augmenter en trois ans ? Ici $P = 1000$, $i = 0{,}07$ et $n = 3$. Le symbole A représente la somme obtenue au bout des trois années. La formule des intérêts composés nous donne A = 1 225,04 €.

Le compte de Simon lui rapporte toujours les mêmes intérêts, à savoir 7 % en intérêts simples. Comment ses bénéfices vont-ils évoluer au bout de trois ans ? La première année, ses intérêts s'élèvent à 70 € et c'est la même chose la deuxième et la troisième année. Il a donc 3 × 70 € d'intérêts, ce qui équivaut à une somme totale de 1 210 € au bout des trois ans. L'investissement de Charles est un meilleur choix financier.

Des sommes d'argent qui augmentent par composition des intérêts peuvent s'accroître très rapidement. C'est très bien si vous économisez mais beaucoup moins bien si vous empruntez. Un élément clé des intérêts composés est la longueur de la période durant laquelle les intérêts sont calculés. Charles a entendu parler d'un placement qui génère 1 % par semaine, soit un centime pour chaque euro. Combien peut-il gagner avec ce système ?

Simon pense connaître la réponse : il suggère de faire le produit du taux d'intérêt 1 % par 52 (nombre de semaines dans l'année) et obtient un taux annuel de 52 %. Cela signifie que les intérêts s'élèvent à 520 €, soit un total de 1 520 €. Charles lui rappelle cependant la magie des intérêts composés et la formule qui s'y rapporte. Avec P = 1 000 €, $i = 0{,}01$ et $n = 52$, Charles calcule et trouve 1 000 € × $(1{,}01)^{52}$. Sa calculatrice lui donne un résultat égal à 1 677,69 €, ce qui est bien supérieur à la

1718
Abraham de Moivre étudie les statistiques de mortalité et le fondement de la théorie des annuités.

1756
James Dodson publie *First Lectures on Insurances*.

1848
L'Institut des Actuaires est fondé à Londres.

somme de Simon. Le taux annuel équivalent de Charles est de 67,769 %, ce qui est beaucoup plus que les 52 % de Simon.

Simon est impressionné mais son argent est déjà placé à la banque sous le régime des intérêts simples. Il se demande combien de temps il lui faudra pour doubler son capital initial de 1 000 €. Chaque année, il a 70 € d'intérêts. Il lui suffit donc de diviser 1 000 par 70. Il obtient 14,29 et il peut alors être sûr que dans 15 ans, il aura plus de 2 000 € à la banque. C'est long. Pour montrer la supériorité des intérêts composés, Charles commence à calculer la période nécessaire pour doubler son capital. C'est un peu plus compliqué mais un ami lui parle de la règle de 72.

La règle de 72 Pour un taux donné, la règle de 72 est une règle approximative pour estimer le nombre de périodes nécessaires pour doubler le capital. Charles s'intéresse à des périodes d'un an, mais la règle de 72 s'applique aussi à des périodes de plusieurs jours ou plusieurs mois. Pour trouver la période nécessaire qui lui permettra de doubler son capital, Charles doit simplement diviser 72 par le taux d'intérêt.

Le calcul est le suivant : 72/7 = 10,3 et donc Charles peut dire à son frère que son investissement doublera en 11 ans, autrement dit, bien plus rapidement que celui de Simon qui doublera en 15 ans. Cette règle donne peut-être une approximation mais elle se révèle utile lorsqu'il faut prendre des décisions rapides.

Valeur présente Le père de Charles est si impressionné par le bon sens de son fils qu'il le prend à part et lui dit : « Je te propose de te donner 100 000 € ». Charles est fou de joie. Son père ajoute ensuite qu'il lui donnera les 100 000 € à son quarante-cinquième anniversaire, dans 10 ans. Charles est déjà moins heureux.

Charles veut dépenser l'argent maintenant mais, manifestement, c'est impossible. Il se rend à sa banque et leur promet les 100 000 € dans 10 ans. La banque répond que le temps, c'est de l'argent, et que 100 000 € dans 10 ans, ce n'est pas la même chose que 100 000 € maintenant. La banque doit évaluer l'investissement nécessaire aujourd'hui pour atteindre la somme de 100 000 € dans 10 ans. C'est ce qu'ils prêteront à Charles. La banque pense qu'un taux de croissance de 12 % leur rapporterait un bon bénéfice. Quelle somme déposée aujourd'hui atteindrait 100 000 € dans dix ans, avec un taux d'intérêt de 12 % ? On peut également utiliser la formule des intérêts composés pour résoudre ce problème . Cette fois, on nous donne A = 100 000 € et il s'agit de calculer P, valeur présente de A. Avec $n = 10$ et $i = 0{,}12$, la banque sera prête à avancer à Charles la somme de $100\,000 / 1{,}12^{10} = 32\,197{,}32$ €. Celui-ci trouve cette somme scandaleusement petite, mais il pourra quand même l'acheter, cette superbe Porsche dont il rêve.

Comment gérer des paiements réguliers ? Maintenant que le père de Charles a promis de donner 100 000 € à son fils dans 10 ans, il doit économiser. C'est ce qu'il a l'intention de faire au moyen d'une succession de versements égaux effectués à la fin de chaque année pendant 10 ans. À la fin de la période, il sera alors en mesure de remettre l'argent à Charles le jour promis, et Charles pourra apporter l'argent à la banque pour rembourser le prêt.

Le père de Charles réussit à trouver un placement qui lui permet de procéder ainsi, placement qui rapporte un taux annuel de 8 % pendant les 10 ans. Il demande à Charles de calculer les versements annuels. Avec la formule des intérêts composés, Charles ne s'occupait que d'un versement (le versement initial) mais il lui faut maintenant prendre en compte dix versements effectués à des moments différents. Si les versements réguliers R sont effectués à la fin de chaque année dans un contexte où le taux d'intérêt est i, la somme épargnée après n années peut être calculée avec la formule des versements réguliers.

$$S = R \times \frac{((1+i)^n - 1)}{i}$$

Formule des versements réguliers

Charles sait que S = 100 000 €, n = 10 et i = 0,08 et il trouve R = 6 902,95 €.

Maintenant que Charles possède sa Porsche flambant neuve, avec la permission de la banque, il a besoin d'un garage. Il décide de faire un emprunt de 300 000 € pour acheter une maison, somme qu'il remboursera en une succession de versements annuels égaux pendant 25 ans. Il assimile cette situation à un problème où les 300 000 € représentent la valeur présente d'une succession de versements à effectuer et il calcule facilement ses versements annuels. Son père est impressionné et utilise encore le talent de Charles. Il vient juste de recevoir un capital retraite de 150 000 € et veut acheter un viager. « Pas de problème, » répond Charles, « on peut utiliser la même formule puisque le problème mathématique est le même. Au lieu de demander à la société de prêts d'avancer de l'argent qui est remboursé par traites échelonnées, tu leur donnes l'argent et ils te font des versements réguliers. »

Au fait, la réponse au casse-tête d'Henry Dudeney est 130 €, soit les 51 € que Norman a donnés au client auxquels s'ajoutent les 79 € qu'il a versés pour acheter le vélo.

l'idée clé
Les intérêts composés sont les meilleurs

45 Le problème du régime

Tanya Smith prend sa forme physique très au sérieux. Elle fait de la gym chaque jour et surveille son régime attentivement. Elle se débrouille dans la vie en travaillant à temps partiel et doit faire attention à ses dépenses. Il est crucial pour elle de prendre la bonne quantité de minéraux et de vitamines chaque mois pour rester en pleine forme. Ces quantités ont été déterminées par son entraîneur. Selon lui, les futurs champions olympiques devraient avoir un apport mensuel minimum de 120 mg en vitamines et de 880 mg en minéraux. Pour être sûre de bien suivre ce régime, Tanya a recours à deux compléments alimentaires. L'un, sous forme solide, s'appelle Solido, tandis que l'autre, sous forme liquide, est commercialisé sous le nom de Liquex. Il s'agit pour elle de décider de la quantité de chaque produit qu'il lui faudra acheter chaque mois pour respecter le souhait de son entraîneur.

Le problème classique du régime consiste à avoir une alimentation saine tout en dépensant le moins possible. C'était un prototype des problèmes de programmation linéaire, domaine développé dans les années 1940 et qui a aujourd'hui de nombreux champs d'applications différents.

Début mars, Tanya se rend au supermarché et vérifie la composition de Solido et de Liquex. Au dos d'un paquet de Solido, elle découvre qu'il contient 2 mg de vitamines et 10 mg de minéraux, alors qu'une brique de Liquex contient 3 mg de vitamines et 50 mg de minéraux. Elle remplit consciencieusement son caddie de 30 boîtes de Solido et de 5 briques de Liquex pour le mois. Mais alors qu'elle se dirige vers la caisse, elle se demande si elle a pris les quantités suffisantes. Elle commence par calculer la quantité de vitamines que contient son caddie. Dans les 30 paquets de Solido, elle a $2 \times 30 = 60$ mg de vitamines et dans le Liquex, $3 \times 5 = 15$. En tout, elle a

	Solido	Liquex	Besoins
Vitamines	2 mg	3 mg	120 mg
Mineraux	10 mg	50 mg	880 mg

chronologie

1826
Fourier anticipe la programmation linéaire ; Gauss résout des équations linéaires par l'élimination Gaussienne.

1902
Farkas donne une solution aux systèmes d'inéquations.

$2 \times 30 + 3 \times 5 = 75$ mg de vitamines. Elle procède de même pour les minéraux et trouve $10 \times 30 + 50 \times 5 = 550$ mg de minéraux.

Puisque son entraîneur a exigé qu'elle prenne au moins 120 mg de vitamines et 880 mg de minéraux, il lui faut remplir son caddie de davantage de boîtes et de briques. Le problème pour Tanya est de se débrouiller pour calculer les bonnes quantités des deux produits de manière à couvrir ses besoins en vitamines et minéraux. Elle revient dans le rayon des produits diététiques et ajoute des boîtes et des briques dans son caddie. Elle a maintenant 40 boîtes et 15 briques. C'est sûrement assez ? Elle refait ses calculs : elle a $2 \times 40 + 3 \times 15 = 125$ mg de vitamines et $10 \times 40 + 50 \times 15 = 1\,150$ mg de minéraux. Tanya respecte maintenant les recommandations de son entraîneur et a même dépassé les quantités nécessaires.

Des solutions réalisables Cette combinaison (40, 15) de produits diététiques permettra à Tanya de respecter son régime. C'est ce que l'on appelle une combinaison possible, ou une solution « réalisable ». Nous avons déjà vu que (30, 5) n'est pas une solution réalisable et il faut donc distinguer entre les deux types de combinaisons, à savoir, des solutions réalisables où le régime est respecté, et des solutions non réalisables où il ne l'est pas.

Tanya a beaucoup d'autres possibilités. Elle pourrait remplir son caddie de Solido uniquement. Dans ce cas, il lui faudrait en acheter au moins 88 boîtes. L'achat (88, 0) respecte les deux exigences, parce que cette combinaison contient $2 \times 88 + 3 \times 0 = 176$ mg de vitamines et $10 \times 88 + 50 \times 0 = 880$ mg de minéraux. Si elle n'achetait que du Liquex, elle aurait besoin de 40 briques au moins, et la solution réalisable (0, 40) respecte à la fois ses besoins en vitamines et en minéraux, parce que $2 \times 0 + 3 \times 40 = 120$ mg de vitamines et $10 \times 0 + 50 \times 40 = 2\,000$ mg de minéraux. On peut remarquer que la prise de vitamines et de minéraux ne correspond pas exactement à ce qui est recommandé quelle que soit la combinaison retenue parmi toutes ces possibilités, mais l'entraîneur aura malgré tout la conviction que Tanya en absorbe suffisamment.

Solutions optimales L'argent entre maintenant en ligne de compte. Lorsque Tanya arrive à la caisse, elle doit régler ses achats. Elle remarque que les boîtes et les briques coûtent 5 € l'unité. Avec les combinaisons réalisables que nous avons trouvées jusque-là (40, 15), (88, 0) et (0, 40), il lui faudrait respectivement payer 275 €, 440 € et 200 €, et la meilleure solution est par conséquent de ne pas acheter de Solido mais 40 briques de Liquex. C'est l'achat le moins coûteux qui respecte ses besoins nutritionnels. Mais la quantité de produits à acheter a été déterminée de manière hasardeuse. Tanya a essayé instinctivement diverses combinaisons de Solido et de Liquex, puis elle a calculé le prix de ces seuls cas. Peut-elle mieux faire ?

1945
Stigler résout le problème du régime selon une méthode heuristique.

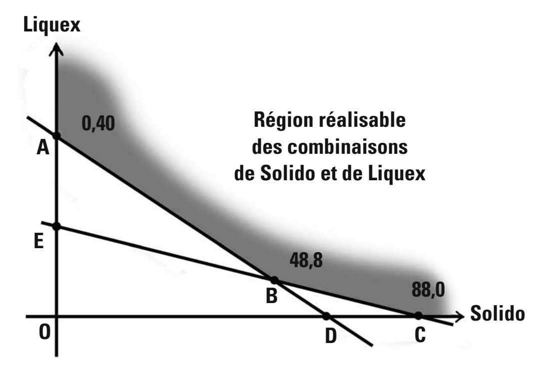
1947
Dantzig formule la méthode du simplexe et résout le problème du régime par la technique de la programmation linéaire.

1984
Karmarkar conçoit un nouvel algorithme pour résoudre les problèmes de programmation linéaire.

Existe-t-il une combinaison possible de Solido et de Liquex qui puisse satisfaire son entraîneur et en même temps lui coûter le moins cher possible ? Ce qu'elle aimerait faire, c'est rentrer chez elle, prendre un papier et un crayon, et étudier le problème.

Problèmes de programmation linéaire On a toujours appris à Tanya à visualiser ses objectifs. Si elle est capable d'appliquer cette technique pour gagner une médaille d'or aux Jeux Olympiques, pourquoi ne pourrait-elle pas faire pareil en mathématiques ? Elle trace alors un schéma de la région réalisable. C'est possible parce qu'elle ne prend en compte que deux aliments. La droite (AD) représente les combinaisons de Solido et de Liquex qui contiennent exactement 120 mg de vitamines. Les combinaisons au-dessus de cette droite contiennent plus de 120 mg de vitamines. La droite (EC) représente les combinaisons qui contiennent exactement 880 mg de minéraux. Les combinaisons d'aliments qui se trouvent au-dessus de ces deux droites correspondent à la région réalisable et représentent toutes les combinaisons réalisables que Tanya peut acheter.

Les problèmes de ce type sont appelés des problèmes de programmation linéaire. Le terme « programmation » signifie qu'il y a une procédure (aujourd'hui, il est devenu synonyme de programme informatique) tandis que « linéaire » fait référence à l'utilisation de droites. Pour résoudre le problème de Tanya avec la programmation linéaire, les mathématiciens ont montré qu'il suffit de calculer à combien s'élèvera la note de Tanya aux points situés aux sommets du polygone des contraintes. Tanya a découvert une autre solution réalisable au point *B* de coordonnées (48, 8) : elle pourrait acheter 48 boîtes de Solido et 8 briques de Liquex. Dans ce cas, elle respecterait parfaitement son régime parce que cette combinaison contient 120 mg de vitamines et 880 mg de minéraux. Au prix de 5 € la boîte et la brique, cette combinaison lui reviendrait à 280 €. L'achat optimal reste donc ce qu'il était auparavant, c'est-à-dire qu'elle ne devrait pas acheter de Solido mais acheter 40 briques de Liquex pour un coût total de 200 €, même si elle a ainsi 1 120 mg de minéraux en trop par rapport aux 880 mg dont elle a besoin.



La combinaison optimale dépend en définitive du prix des produits. Si le prix des boîtes de Solido passait à 2 € et celui de Liquex à 7 €, alors les combinaisons des points *A* (0, 40), *B* (48,8) et *C* (88, 0) coûteraient respectivement 280 €, 152 €, et 176 €.

La meilleure solution pour Tanya dans ce dernier cas est d'acheter 48 boîtes de Solido et 8 briques de Liquex, pour un coût total de 152 €.

Histoire En 1947, le mathématicien américain George Dantzig, qui travaillait alors pour l'armée de l'air américaine, mit au point une méthode appelée « méthode

du simplexe » pour résoudre les problèmes de programmation linéaire. Ce fut une telle réussite que Dantzig fut reconnu en Occident comme le père de la programmation linéaire. Dans la Russie Soviétique, qui était coupée du monde pendant la Guerre Froide, Leonid Kantorovich et le mathématicien hollandais Tjalling Koopmans reçurent le Prix Nobel d'économie pour leurs travaux sur l'allocation des ressources par la technique de la programmation linéaire.

Tanya ne traitait que deux aliments, deux variables, mais aujourd'hui, les problèmes qui impliquent des milliers de variables sont assez communs. Lorsque Dantzig découvrit sa méthode, il y avait peu d'ordinateurs mais le « Projet des Tables Mathématiques » était lancé, programme commencé à New York en 1938 qui nécessita dix ans de travail. Une équipe de quelque dix calculateurs humains travaillèrent pendant 12 jours pour résoudre un problème de régime avec neuf « vitamines » et 77 variables.

Alors que la méthode du simplexe et ses variantes sont une réussite phénoménale, d'autres méthodes furent également essayées. En 1984, le mathématicien indien Narendra Karmarkar conçut un nouvel algorithme de portée pratique, et le russe Leonid Khachiyan en proposa une autre qui présentait surtout un intérêt théorique.

On a appliqué le modèle de base de la programmation linéaire à de nombreuses autres situations que celle du choix d'un régime. Dans le problème du transport par exemple, il s'agit du transport de produits manufacturés vers des entrepôts. Avec sa structure spéciale, il est devenu une véritable branche de la programmation linéaire à lui tout seul. Dans ce type de problème, il faut réduire au maximum le coût du transport. Dans certains problèmes de programmation linéaire, on recherche la maximisation (comme pour un profit). Dans d'autres problèmes, les variables ne prennent que des valeurs entières ou les deux valeurs 0 ou 1 seulement, mais ces problèmes sont assez différents et font appel à des procédures de résolution particulières.

Il reste à voir si Tanya Smith gagnera la médaille d'or aux Jeux Olympiques. Si elle y parvient, ce sera un triomphe de plus pour la programmation linéaire.

l'idée clé
Garder la santé à tout prix

46 Le voyageur de commerce

James Cook, qui travaille dans une agence de Bismarck (Dakota-du-Nord, États-Unis), est un excellent voyageur de commerce qui vend un nettoyant spécial moquettes pour l'entreprise Electra. Le fait qu'il ait été désigné vendeur de l'année trois fois de suite atteste de son savoir-faire. Son secteur de vente comprend Albuquerque, Chicago, Dallas et El paso, et il se rend dans chacune de ces villes une fois par mois lors d'un déplacement unique. Son problème est de savoir comment effectuer ce déplacement tout en minimisant la distance totale parcourue. C'est le problème classique du voyageur de commerce.

James a tracé un graphique des distances qui séparent les villes. Bismarck est par exemple à 1 641 km de Dallas, comme l'indique la cellule grisée à l'intersection de la colonne de Bismarck et de la ligne de Dallas.

La méthode gloutonne Pragmatique, James Cook fait un croquis de son secteur de vente qui ne fait pas apparaître les détails mais qui lui donne une représentation globale de la position des villes et de la distance qui les sépare. L'un de ses trajets de prédilection part de Bismarck, passe par Chicago, Albuquerque, Dallas et El Paso avant de revenir à Bismarck. C'est le trajet BCADEB. Mais il se rend compte maintenant que ce trajet de 6 618 km au total a un coût élevé en termes de distance parcourue. Peut-il mieux faire ?

Albuquerque				
1 421	Bismarck			
1 831	1 136	Chicago		
933	1 641	1 263	Dallas	
380	1 770	2 031	948	El Paso

James a certes tracé un plan de son secteur de vente mais il n'a pas envie d'entrer dans le détail : il veut simplement se rendre dans ces villes pour vendre son produit. Il regarde une carte dans son bureau de Bismarck et constate que la ville la plus proche est Chicago. C'est à 1 136 km de Bismarck, alors qu'Albuquerque se trouve à 1 421 km, Dallas à 1 641, et El Paso à 1 770 km. Il se met en route pour Chicago

chronologie

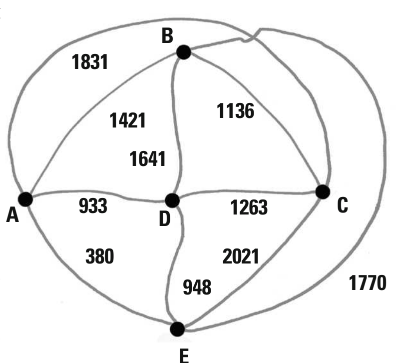
Vers 1810
Charles Babbage cite ce problème qu'il juge intéressant.

1831
Le problème du voyageur de commerce est traité de façon non théorique.

1926
Borůvka introduit l'algorithme glouton.

sans projet préconçu. Arrivé à Chicago, il fait son travail et il cherche la ville la plus proche où il pourra se rendre ensuite. Il choisit Dallas de préférence à Albuquerque et El Paso, parce que c'est à 1 263 km de Chicago, et c'est donc la ville la plus proche de toutes.

Arrivé à Dallas, il a parcouru 1 136 + 1 263 km. Il doit ensuite choisir entre Albuquerque et El Paso. Il opte pour Albuquerque qui est plus proche. D'Albuquerque, il doit se rendre à El Paso, et après quoi, il a vu toutes les villes ; son travail terminé, il revient à Bismarck. Son parcours total est égal à 1 136 +1 263 + 933 + 380 + 1 770 = 5 482 km. Ce trajet BCDAEB est beaucoup plus court que le précédent et a donc aussi produit moins d'émissions carboniques.



Cette façon de faire est souvent appelée la méthode gloutonne de recherche d'un trajet court. Elle est gloutonne parce que la décision de James Cook est toujours locale : il se trouve dans une ville particulière et cherche le meilleur trajet pour quitter cette ville. Avec cette méthode, il n'essaie jamais d'anticiper plus d'une étape à la fois. Cette méthode n'a rien de stratégique parce qu'elle ne tient aucun compte du meilleur trajet. Sa dernière étape étant El Paso, il s'est trouvé obligé de couvrir une longue distance pour revenir à Bismarck. Un trajet plus court a donc été trouvé, mais est-ce le plus court ? James est intrigué.

James voit comment il peut tirer profit du fait que seules cinq villes sont concernées. Le petit nombre de villes permet de dresser la liste de tous les trajets possibles et de choisir ensuite le plus court. Avec cinq villes, il n'y a que 24 trajets à examiner ou seulement 12 si l'on considère qu'un trajet et son inverse sont équivalents. C'est autorisé car tous deux sont de même distance. Cette méthode est bien utile à James Cook car il apprend que le trajet BAEDCB (ou son inverse BCDEAB) est en réalité la solution optimale puisque la distance à parcourir est de 5 147 km seulement.

De retour à Bismarck, James se rend compte que son voyage lui a pris trop de temps. Ce n'est pas la distance qu'il veut réduire, mais le temps. Il trace un nouveau tableau qui donne le temps qui sépare les différentes villes du secteur à parcourir.

Albuquerque				
12 (route)	Bismarck			
6 (avion)	2 (avion)	Chicago		
2 (avion)	4 (avion)	3 (avion)	Dallas	
4 (route)	3 (avion)	5 (avion)	1 (avion)	El Paso

James sait que la somme des distances des deux côtés d'un triangle

1954
Dantzig et Dijkstra proposent des méthodes pour résoudre le problème du voyageur de commerce.

1971
Cook formule le concept *P* versus *NP* pour les algorithmes.

2004
David Applegate résout le problème pour les 24 978 villes de Suède.

est toujours supérieure à la longueur du troisième côté ; dans ce cas, le graphe est dit euclidien et les méthodes de résolution sont bien connues. C'est différent lorsqu'il s'agit de temps. Emprunter les voies aériennes principales est souvent plus rapide que de prendre les voies secondaires et James Cook remarque qu'en allant d'El Paso à Chicago, il est plus rapide de passer par Dallas. Ce que l'on appelle l'inégalité du triangle ne s'applique pas ici.

La méthode gloutonne appliquée au problème du temps donne 22 heures sur le trajet BCDEAB, alors que deux trajets optimaux différents BCADEB et BCDAEB totalisent 14 heures chacun. Le premier est de 6 618 km et le second de 5 482. James Cook se réjouit d'avoir réalisé la plus grande économie en choisissant BCDAEB. Il projette ensuite de réfléchir au trajet le moins onéreux.

Des secondes aux siècles La vraie difficulté que ce problème du voyageur de commerce soulève apparaît lorsqu'il y a un très grand nombre de villes. James Cook est tellement brillant qu'il ne tarde pas à être promu au poste de directeur. Il doit maintenant visiter 13 villes à partir de Bismarck au lieu des 4 villes précédentes. La méthode gloutonne ne lui plaît pas, et il préfère étudier une liste complète des itinéraires possibles. Il entreprend d'en dresser la liste pour ses 13 villes. Il découvre bientôt qu'il n'y aurait pas moins de $3{,}1 \times 10^9$ itinéraires à étudier. En d'autres termes, s'il fallait une seconde pour qu'un ordinateur imprime un itinéraire, il lui faudrait un siècle pour les imprimer tous. Un problème comportant 100 villes occuperait l'ordinateur pendant des milliers d'années.

On a appliqué certaines méthodes sophistiquées au problème du voyageur de commerce. Des méthodes exactes ont été données qui s'appliquent à 5 000 villes ou moins, et l'une d'elles a même permis de traiter un problème particulier de 33 810 villes, en ayant toutefois recours à un ordinateur d'une puissance colossale. Des méthodes inexactes produisent des itinéraires proches de la solution optimale avec une probabilité donnée. Les méthodes de ce type ont l'avantage de permettre de traiter des problèmes concernant des millions de villes.

Complexité algorithmique En nous plaçant du point de vue de l'ordinateur, pensons simplement au temps qu'il lui faudrait pour trouver une solution. Dresser simplement la liste de tous les trajets possibles est le pire scénario. James a découvert qu'avec cette méthode musclée, il faudrait presque un siècle pour 13 villes. Si l'on ajoutait deux villes supplémentaires, on passerait alors à 20 000 ans !

Ces estimations dépendent bien sûr de l'ordinateur utilisé, mais pour n villes, le temps nécessaire augmente proportionnellement à $n!$ (nombre obtenu en multipliant tous les nombres entiers de 1 à n). On a calculé $3{,}1 \times 10^9$ itinéraires pour 13 villes. Déterminer pour chaque itinéraire s'il est le plus court devient un problème de temps *factoriel*… dont la résolution prend du temps.

D'autres méthodes peuvent être utilisées pour résoudre le problème dans lequel le temps pour n villes augmente proportionnellement à 2^n (2 multiplié par lui-même n fois) ; pour 13 villes cela impliquerait donc quelque chose de l'ordre de 8 192

décisions (8 fois plus que pour 10 villes). Un tel algorithme est appelé un algorithme *exponentiel*. Le Saint Graal de ces « problèmes d'optimisation combinatoire » consiste à trouver un algorithme qui dépend non pas de la $n^{ème}$ puissance de 2, mais d'une puissance de *n* fixe. Plus la puissance est faible, mieux c'est ; si l'algorithme variait selon n^2 par exemple, dans le cas des 13 villes, il n'y aurait plus que 169 décisions, autrement dit, moins de deux fois le temps nécessaire pour 10 villes. On dit qu'un tel algorithme est un algorithme *polynomial*, et les problèmes résolus de cette manière sont des « problèmes rapides » dont la résolution peut prendre 3 minutes et non pas des siècles.

Ce genre de problèmes qui peuvent être *résolus* par ordinateur en temps polynomial est désigné par la lettre *P*. On ne sait pas si le problème du voyageur de commerce en fait partie. Personne n'a réussi à produire un algorithme de temps polynomial pour le résoudre, mais personne n'a réussi non plus à montrer qu'il n'en n'existe pas.

Une catégorie plus large notée *NP* est constituée de problèmes dont les solutions peuvent être *vérifiées* en temps polynomial. Le problème du voyageur de commerce en fait certainement partie parce que vérifier qu'un trajet donné est plus court en distance que n'importe quel autre trajet donné peut se faire en temps polynomial. Il vous suffit de faire la somme des distances le long dudit trajet et de comparer le résultat avec le nombre donné. *Trouver* et *vérifier* sont deux opérations différentes : il est par exemple facile de vérifier que $167 \times 241 = 40\,247$ mais trouver les facteurs de 40 247 est une tout autre affaire.

Tout problème vérifiable en temps polynomial (*NP*) peut-il être résolu en temps polynomial (*P*) ? Si c'était vrai, les deux catégories *P* et *NP* seraient identiques et nous pourrions écrire $P = NP$. Savoir si $P = NP$ est actuellement un problème ouvert, et donc délicat, pour les informaticiens. Plus de la moitié de la profession pense que ce n'est pas vrai : ils croient qu'il existe quelque part des problèmes qui peuvent être vérifiés en temps polynomial mais qui ne peuvent pas être résolus en temps polynomial. C'est un problème tellement difficile que l'Institut Mathématique Clay a offert un prix d'un million de dollars pour prouver que $P = NP$ ou $P \neq NP$.

l'idée clé
Trouver le meilleur trajet

47 La théorie des jeux

À en croire certains, Johnny était l'homme le plus intelligent du monde. John von Neumann était un enfant prodige qui devint une légende dans le monde mathématique. Lorsque l'on sut qu'il s'était rendu en taxi à une conférence juste après avoir noté en hâte son « théorème du minimax » de la théorie des jeux, les gens hochèrent simplement la tête. C'était exactement le genre de chose dont von Neumann était capable. Il apporta sa contribution à la mécanique quantique, la logique, l'algèbre, alors pourquoi pas à la théorie des jeux ? De fait, il s'y intéressa de près : il publia avec Oskar Morgenstern l'ouvrage qui fait autorité en la matière, *Théorie des jeux et comportements économiques*. Au sens le plus large, la théorie des jeux existe depuis bien longtemps, mais c'est l'apport décisif de von Neumann qui permit d'affiner la théorie du « jeu à deux joueurs à somme nulle ».

Jeux à deux joueurs à somme nulle Cela paraît compliqué, mais un jeu à deux joueurs à somme nulle est tout simplement un jeu qui « se joue » à deux personnes, deux entreprises ou deux équipes, dans lequel celui qui gagne récupère ce que l'autre perd. Si A gagne 200 €, alors B perd ces 200 € ; c'est ce que l'expression à somme nulle signifie. Il est inutile que A coopère avec B, car c'est de la compétition pure où il n'y a que des gagnants et des perdants. En termes de gains, A gagne 200 € et B gagne – 200 € et la somme est égale à 200 + (– 200) = 0. C'est de là que vient l'expression « à somme nulle ».

Imaginons que deux compagnies de télévision ATV et BTV font une offre pour créer une nouvelle agence de presse en Écosse ou en Angleterre. Chaque compagnie doit faire une offre pour une seule région et leur décision reposera sur l'augmentation de téléspectateurs attendue. Les analystes des médias ont fait une estimation de ces augmentations et les deux compagnies ont accès aux résultats de leurs recherches. Ces résultats sont notés dans une matrice des gains et mesurés en millions de téléspectateurs.

chronologie

1713
Waldergrave donne la première solution mathématique d'un jeu à deux joueurs.

1944
Von Neumann et Morgenstern publient *Théorie des jeux et comportement économique*.

		BTV	
		Écosse	Angleterre
ATV	Écosse	+5	–3
	Angleterre	+2	+4

Si ATV et BTV décident toutes deux de choisir l'Écosse, alors ATV aura un bénéfice de 5 millions de téléspectateurs, mais BTV perdra 5 millions de téléspectateurs. Le signe moins, comme dans le gain – 3, signifie que ATV perdra 3 millions de téléspectateurs. Les gains + sont favorables à ATV et les gains – le sont à BTV.

On admettra que les compagnies se servent de la matrice des gains pour prendre leur décision, et qu'elles font leur offre sous scellé et simultanément. Il est évident que les deux compagnies agissent dans leurs propres intérêts.

Si ATV choisit l'Écosse, le pire serait une perte de 3 millions ; si elle fait une offre pour l'Angleterre, elle aurait au pire un gain de 2 millions. La stratégie évidente pour ATV serait donc de choisir l'Angleterre (ligne 2). Elle ne pourrait pas faire moins bien qu'obtenir un gain de 2 millions de téléspectateurs quel que soit le choix de BTV. En examinant les choses d'un point de vue numérique, ATV trouve – 3 et 2 (les minima par ligne) et choisit la ligne correspondant au maximum.

BTV est dans une position de faiblesse mais peut toujours mettre au point une stratégie qui limite ses pertes potentielles et espérer ainsi une meilleure matrice des gains l'année suivante. Si BTV choisit l'Écosse (colonne 1), elle aurait au pire une perte de 5 millions ; si elle choisit l'Angleterre, le pire serait une perte de 4 millions. La stratégie la plus sûre pour BTV serait de choisir l'Angleterre (colonne 2) car elle préférerait perdre une audience de 4 millions plutôt que de 5 millions. Au pire, elle perdrait 4 millions de téléspectateurs et ce, quelle que soit la décision de ATV.

Ces stratégies seraient les plus sûres pour chaque joueur, et, si elles étaient suivies, ATV aurait un gain de 4 millions de téléspectateurs supplémentaires alors que BTV en perdrait autant.

Un homme d'exception

John Nash (né en 1928) dont la vie agitée a été décrite dans le film *Un homme d'exception* sorti en 2001, reçut le prix Nobel d'économie en 1994 pour ses contributions à la théorie des jeux.

Nash et d'autres avec lui développèrent la théorie des jeux dans le cas où plus de deux joueurs jouent en coopérant, y compris lorsque deux joueurs se liguent contre un troisième. « L'équilibre de Nash » (comme le point-selle) ouvrit de plus larges perspectives que celui de von Neumann, ce qui permit une meilleure compréhension de certaines situations économiques.

1950
Tucker pose le dilemme du prisonnier et Nash propose l'équilibre de Nash.

1982
Maynard Smith publie *L'évolution et la théorie des jeux*.

1994
Nash reçoit le Prix Nobel d'économie pour ses travaux sur la théorie des jeux.

Quand un jeu est-il déterministe ? L'année suivante, les deux compagnies de télé ont une option supplémentaire : le Pays de Galles. Parce que les choses ont changé, une nouvelle matrice des gains est établie.

		BTV			
		Pays de Galles	Écosse	Angleterre	Minimum par ligne
ATV	Pays de Galles	+3	+2	+1	+1
	Écosse	+4	−1	0	−1
	Angleterre	−3	+5	−2	−3
	Maximum par colonne	+4	+5	+1	

Comme auparavant, la stratégie la plus sûre pour ATV est de choisir la ligne qui maximise le pire résultat possible. Le maximum des gains minimums {+ 1, – 1, – 3} est le Pays de Galles. La stratégie la plus sûre pour BTV est de choisir la colonne qui minimise les gains maximums {+ 4, + 5, + 1}. C'est l'Angleterre (colonne 3).

En choisissant le Pays de Galles, ATV peut être sûre de ne pas gagner moins d'1 million de téléspectateurs quelle que soit la décision de BTV, et en choisissant l'Angleterre (colonne 3), BTV peut s'assurer de ne pas perdre plus d'1 million de téléspectateurs quelle que soit la décision d'ATV. Ces choix représentent donc les meilleures stratégies pour chaque compagnie, et en ce sens, le jeu est déterministe (mais il reste injuste pour BTV). Dans ce jeu,

$$\text{maximum de } \{+1, -1, -3\} = \text{minimum de } \{+4, +5, +1\}$$

et chaque côté de l'équation a pour valeur commune + 1. Contrairement au premier jeu, cette version a un « point-selle » d'équilibre qui est + 1.

Jeux répétitifs Le jeu répétitif par excellence est le jeu traditionnel du « Chi-Fou-Mi ». Contrairement aux jeux des compagnies de télé qui ne se jouaient qu'une seule fois, ce jeu est habituellement joué une demi-douzaine de fois, ou quelques centaines de fois lors des Championnats Mondiaux annuels.

Dans ce jeu, deux joueurs présentent une main, deux doigts ou un poing qui symbolisent respectivement du papier, une paire de ciseaux ou une pierre. Ils jouent en même temps après avoir compté jusqu'à 3 : le papier fait match nul avec le papier, il est battu par les ciseaux (parce que les ciseaux le coupent), mais il bat la pierre (parce qu'il peut l'envelopper). Si l'on joue « papier », les gains sont donc 0, – 1, + 1, ce qui correspond à la ligne supérieure de notre matrice des gains.

	papier	ciseaux	pierre	Minimum par ligne
papier	Égalité = 0	Perd = – 1	Gagne = + 1	−1
ciseaux	Gagne = + 1	Égalité = 0	Perd = – 1	−1
pierre	Perd = – 1	Gagne = +	Égalité = 0	−1
Maximum par colonne	+1	+1	+1	

Il n’y a pas de point-selle pour ce jeu, et aucune stratégie véritable ne se dégage de manière évidente. Si un joueur choisit toujours le papier par exemple, son adversaire s’en rendra compte et il lui suffira de choisir les ciseaux pour gagner à chaque fois. Selon le « théorème du minimax » de von Neumann, il existe une « stratégie mixte » c’est-à-dire une façon de choisir différentes actions qui repose sur les probabilités.

D’un point de vue mathématique, les joueurs devraient faire leur choix de manière aléatoire, mais globalement, le papier, les ciseaux et la pierre devraient tous être choisis avec une probabilité égale à 1/3. Toutefois, s’en remettre aveuglément au hasard n’est peut-être pas toujours la meilleure ligne de conduite à adopter. Les champions du monde ont en effet une façon particulière de choisir leur stratégie qui consiste à utiliser une petite astuce « psychologique ». Ils sont très doués pour anticiper les réactions de leurs adversaires.

À quel moment un jeu n’est-il pas à somme nulle ? Tous les jeux ne sont pas à somme nulle. Chaque joueur possède parfois sa propre matrice des gains. Un exemple célèbre est le dilemme du « prisonnier » conçu par A. W. Tucker.

Deux hommes, André et Bernard, sont arrêtés par la police sur présomption de vol caractérisé et détenus dans des cellules séparées de manière à éviter tout échange entre eux. Les gains, lorsqu’il s’agit comme ici de condamnations à la prison, ne dépendent pas seulement des réactions des accusés lors des interrogatoires de police mais aussi de la manière dont ils répondent conjointement. Si **A** avoue et si **B** nie, alors **A** est condamné à un an de prison (de la matrice des gains de **A**) mais **B** est condamné à 10 ans (de la matrice des gains de **B**). Si **A** n’avoue pas mais si **B** avoue, les condamnations s’inversent. Si tous les deux avouent, ils sont condamnés à 4 ans chacun, mais si aucun n’avoue et qu’ils clament tous deux leur innocence, ils s’en sortent indemnes !

A		**B**	
		Avoue	N’avoue pas
A	Avoue	+4	+1
	N’avoue pas	+10	0

B		**B**	
		Avoue	N’avoue pas
A	Avoue	+4	+10
	N’avoue pas	+1	0

Si les prisonniers pouvaient coopérer, ils prendraient la ligne de conduite optimale et n’avoueraient pas : ce serait un accord « gagnant-gagnant ».

l’idée clé
Mathématiques gagnant-gagnant

48 La relativité

Lorsqu'un objet se déplace, on mesure son mouvement par rapport à d'autres objets. Si l'on roule à 100 km/h et que, sur la même route, une autre voiture roule à 100 km/h dans la même direction, notre vitesse relative par rapport à cette voiture est nulle. Et pourtant, nous roulons tous les deux à 100 km/h par rapport au sol. Et notre vitesse est de 200 km/h par rapport à une voiture qui roule à 100 km/h en sens inverse. La théorie de la relativité a changé notre manière de penser.

La théorie de la relativité a été conçue par le physicien hollandais Hendrik Lorentz à la fin du XIX[e] siècle, mais des progrès décisifs furent accomplis par Albert Einstein en 1905. Son célèbre article sur la relativité restreinte a révolutionné l'étude de la manière dont les objets se déplacent, réduisant la théorie classique de Newton, découverte magnifique en son temps, à un cas particulier.

Retour à Galilée Pour décrire la théorie de la relativité, allons trouver le maître lui-même : Einstein adorait parler des trains qui l'inspiraient pour mener ses expériences. Dans notre exemple, Jean Darmond est dans un train de banlieue qui circule à 60 km/h. Il quitte son siège à l'arrière du train et se rend au wagon-restaurant à 2 km/h. Sa vitesse est de 62 km/h par rapport au sol. En revenant à sa place, la vitesse relative de Jean par rapport au sol est de 58 km/h parce qu'il marche dans la direction opposée à celle du train. C'est ce que la théorie de Newton nous dit. La vitesse est un concept relatif et c'est le sens du déplacement de Jean qui nous dit s'il faut additionner ou soustraire.

Parce que tout mouvement est relatif, on parle d'un « référentiel » qui est le point à partir duquel on mesure un déplacement particulier. En ce qui concerne le déplacement à une seule dimension du train qui suit une voie rectiligne, on peut se représenter un référentiel fixe situé dans une gare, une distance x et un moment t tous deux repérés relativement à ce référentiel. La position zéro est déterminée par un point noté sur le quai et le temps est indiqué sur l'horloge de la gare. Les coordonnées distance/temps relativement au référentiel choisi sont (x, t).

Il y a aussi un référentiel dans le train. Si l'on mesure la distance depuis l'arrière du train et l'heure à la montre de Jean, on a un autre couple de coordonnées $(\overline{x}, \overline{t})$.

chronologie

Vers 1632
Galilée donne les « transformations de Galilée » pour expliquer la chute des corps.

1676
Römer calcule la vitesse de la lumière à partir de l'observation des satellites de Jupiter.

1687
Newton décrit dans son ouvrage *Principia* les lois classiques du mouvement.

Il est aussi possible de synchroniser ces deux systèmes de coordonnées. Lorsque le train passe à côté du repère sur le quai, alors $x = 0$ et l'horloge de la gare est à $t = 0$. Si Jean pose $\bar{x} = 0$ cet endroit et $\bar{t} = 0$ à sa montre, il y a maintenant un lien entre ces coordonnées.

Alors que le train passe dans la gare, Jean se lève pour se rendre au wagon-restaurant. On peut calculer la distance qui le sépare de la gare 5 minutes plus tard. On sait que le train roule à 1 km par minute, et donc pendant cette durée, il a effectué 5 kilomètres alors que, dans le même temps, Jean a parcouru une distance de $\bar{x} = 10/60$ km (résultat obtenu à partir de sa vitesse de 2 km/h multipliée par le temps 5/60). Donc au total, Jean est à une distance (x) située à 5 + 10/60 kilomètres de la gare. Le rapport entre x et $\bar{x}$ est donc donné par $x = \bar{x} + v \times t$ (ici $v = 60$). Si l'on inverse l'équation pour donner la distance que Jean a parcourue par rapport au référentiel dans le train, on obtient

$$\bar{x} = x - v \times t.$$

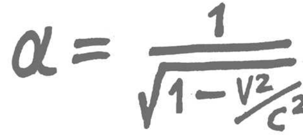
Le concept du temps dans la théorie classique de Newton est un flux à une seule dimension qui se dirige du passé vers le futur. Il est universel pour tous et il ne dépend pas de l'espace. Parce que c'est une quantité absolue, le temps de Jean dans le train est le même pour le chef de gare resté sur le quai t, et donc

$$\bar{t} = t.$$

Ces deux formules pour $\bar{x}$ et $\bar{t}$, d'abord trouvées par Galilée, sont des équations appelées transformations, parce qu'elles font passer les quantités d'un référentiel à un autre. Selon la théorie classique de Newton, on devrait s'attendre à ce que la vitesse de la lumière obéisse à ces deux transformations galiléennes pour $\bar{x}$ et $\bar{t}$.

Dès le XVII[e] siècle, on admettait que la lumière avait une vitesse dont la valeur approximative fut mesurée en 1676 par l'astronome danois Ole Römer. Lorsqu'Albert Michelson mesura la vitesse de la lumière plus précisément en 1881, il trouva qu'elle était de 299 821 km par seconde. Il fit même mieux en prenant conscience de la différence entre la transmission de la lumière et de celle du son. Michelson trouva que, contrairement à la vitesse de notre observateur dans le train en mouvement, la direction du rayon de lumière n'était en rien relative à la vitesse de la lumière. Il était nécessaire d'expliquer ce résultat paradoxal.

La théorie de la relativité restreinte Lorentz mit au point les équations mathématiques qui gouvernent le lien entre la distance et le temps lorsqu'un référentiel se déplace à vitesse constante v par rapport à un autre. Ces transformations sont très semblables à celles que nous avons déjà trouvées mais impliquent un facteur, appelé facteur de



Le facteur de Lorentz

1881
Michelson mesure la vitesse de la lumière avec une grande précision.

1887
Les transformations de Lorentz sont formulées.

1905
Einstein publie *Sur l'électrodynamique des corps en mouvement*, article qui décrit la relativité restreinte.

1915
Einstein publie *The field equations for gravitation* sur la relativité générale.

Lorentz et noté α, qui dépend de v et de la vitesse de la lumière dans le vide notée c (du latin « *celeritas* », la célérité).

Einstein entre en scène Einstein se servit des découvertes de Michelson sur la vitesse de la lumière pour en faire un postulat :

La vitesse de la lumière est constante pour tous les observateurs quelle que soit la direction.

Si Jean Darmond allumait et éteignait une torche dans le train en passant dans la gare, et s'il dirigeait le faisceau lumineux dans le sens de déplacement du train, il lui trouverait une vitesse égale à c. Le postulat d'Einstein dit que le chef de gare posté sur le quai trouverait aussi que la vitesse du faisceau est égale à c, et non à c + 60 km/h. Einstein posa également un deuxième principe :

Un référentiel se déplace avec une vitesse constante par rapport à un autre.

Le génie de l'article d'Einstein de 1905 tient en partie à la manière dont il aborda le problème, guidé par l'élégance mathématique. Les ondes du son voyagent sous forme de vibrations de molécules dans le milieu où le son se propage. D'autres physiciens avaient supposé que la lumière avait elle aussi besoin d'un milieu particulier pour se propager. Personne ne savait de quoi il s'agissait, mais on lui donna un nom : l'éther luminifère.

Einstein ne trouva pas nécessaire de supposer l'existence de cet espace comme milieu de transmission de la lumière. Au lieu de cela, il déduisit les transformations de Lorentz à partir des deux principes simples de la relativité, ce qui permit à la théorie de s'épanouir entièrement. Il montra en particulier que l'énergie d'une particule E est déterminée par l'équation $E = \alpha \times mc^2$. Pour l'énergie d'un corps au repos (lorsque $v = 0$ et que donc $\alpha = 1$), cela débouche sur la célèbre équation qui montre que la masse et l'énergie sont proportionnelles :

$$E = mc^2.$$

Lorentz et Einstein furent tous deux proposés pour le prix Nobel de 1912. Lorentz l'avait déjà reçu en 1902, mais Einstein dut attendre 1921 pour être finalement récompensé pour son travail sur l'effet photoélectrique (qu'il avait aussi publié en 1905). Ce fut une année vraiment miraculeuse pour le petit employé suisse.

Einstein contre Newton Lorsqu'il s'agit de trains qui se déplacent à faible vitesse, il y a peu de différence entre la théorie de la relativité d'Einstein et la théorie classique de Newton. Dans ces exemples, la vitesse relative v est si petite par rapport à celle de la lumière que le facteur de Lorentz α est proche de 1. Les équations de Lorentz sont dans ce cas virtuellement les mêmes que les transformations classiques de Galilée. Par conséquent, Einstein et Newton seraient d'accord lorsqu'il s'agit de vitesses faibles. Il faut que les vitesses et les distances soient très grandes pour qu'apparaissent les différences entre les deux théories. Même le TGV, qui bat tous les records de vitesse, n'est pas encore allé aussi vite, et ce n'est pas demain que les progrès réalisés dans les transports ferroviaires nous obligeront à écarter la théorie de Newton au profit de celle d'Einstein. Ce sont les voyages dans l'espace qui nous y obligeront.

La théorie de la relativité générale Einstein publia sa théorie générale en 1915. Cette théorie s'applique au mouvement lorsque les référentiels peuvent accélérer les uns par rapport aux autres et elle fait le lien entre les effets de l'accélération et ceux de la gravitation.

Grâce à la théorie générale, Einstein fut capable de prédire un phénomène physique tel que la déformation des rayons lumineux par les champs gravitationnels de gros objets comme le Soleil. Sa théorie explique aussi le mouvement de l'axe de rotation de Mercure. Cette précession n'a pas été complètement expliquée par la théorie de la gravitation de Newton et il en va de même pour la force exercée sur Mercure par les autres planètes. Ce problème embarrassait les astronomes depuis les années 1840.

Le référentiel de la théorie générale est l'espace-temps à quatre dimensions. L'espace d'Euclide est plat (il a une courbure nulle) mais la géométrie de l'espace-temps à quatre dimensions d'Einstein (ou la géométrie Riemannienne) est courbe. Elle remplace la force de gravitation Newtonienne pour expliquer l'attraction des objets entre eux. Avec la théorie de la relativité générale d'Einstein, c'est la courbure de l'espace-temps qui explique cette attraction. En 1915, Einstein provoqua une nouvelle révolution scientifique.

l'idée clé
La vitesse de la lumière est absolue

49 Le grand théorème de Fermat

La somme de deux carrés peut parfois donner un troisième carré. Par exemple, $5^2 + 12^2 = 13^2$. Mais peut-on faire la somme de deux cubes et obtenir un autre cube ? Qu'en est-il des puissances plus élevées ? Chose étonnante, c'est impossible. Le grand théorème de Fermat stipule que pour tous nombres entiers *x*, *y*, *z* et *n*, l'équation $x^n + y^n = z^n$ n'a pas de solution non triviale lorsque *n* est strictement supérieur à 2. Fermat affirma avoir trouvé une « démonstration merveilleuse » de cette proposition, torturant ainsi des générations de mathématiciens mais également un enfant de 10 ans qui lut un jour un livre emprunté à la bibliothèque municipale sur cette chasse au trésor mathématique.

Le grand théorème de Fermat porte sur une équation diophantienne, équation dont la résolution constitue un défi des plus coriaces à relever. Les solutions de ces équations doivent être des nombres entiers. Elles tiennent leur nom de Diophante d'Alexandrie dont l'ouvrage *Arithmetica* devint un outil incontournable de la théorie des nombres. Pierre de Fermat était magistrat dans la ville de Toulouse. Mathématicien aux multiples talents, il était surtout connu pour ses travaux éclairés dans la théorie des nombres, et on se souvient tout particulièrement de lui pour avoir énoncé le grand théorème qui porte son nom, sa dernière contribution aux mathématiques. Fermat le démontra, ou pensa l'avoir démontré, et écrivit dans son exemplaire d'*Arithmetica* de Diophante : « J'ai trouvé une démonstration vraiment merveilleuse de cette proposition mais la marge est trop étroite pour la contenir. »

Fermat a résolu de nombreux grands problèmes exception faite de son grand théorème, semble-t-il. Ce théorème a occupé des légions de mathématiciens pendant 300 ans, et n'a été prouvé que très récemment. Aucune marge ne pouvait contenir une telle preuve et les techniques modernes nécessaires pour la produire jettent un doute énorme sur l'affirmation de Fermat.

chronologie

Vers 1665
Fermat décède, sans laisser de trace de sa « démonstration merveilleuse ».

1753
Euler prouve le cas pour $n = 3$.

1825
Legendre et Dirichlet prouvent séparément le cas pour $n = 5$.

1839
Lamé prouve le cas pour $n = 7$.

L'équation $x + y = z$ Comment résoudre cette équation avec trois variables x, y et z ? Dans une équation, on a d'ordinaire une inconnue x, mais ici, il y en a 3. Cela permet en fait de résoudre facilement l'équation $x + y = z$. On peut choisir les valeurs de x et y comme on veut, en faire la somme pour obtenir z et ainsi obtenir une solution. C'est aussi simple que cela.

Si l'on choisit par exemple $x = 3$ et $y = 7$, les valeurs $x = 3$, $y = 7$ et $z = 10$ sont solutions de l'équation. Cela permet aussi de voir que certaines valeurs de x, y et z ne sont pas solutions de l'équation. Par exemple, $x = 3$, $y = 7$ et $z = 9$ ne sont pas solutions de l'équation parce qu'avec ces valeurs, la somme $x + y$ n'est pas égale à z.

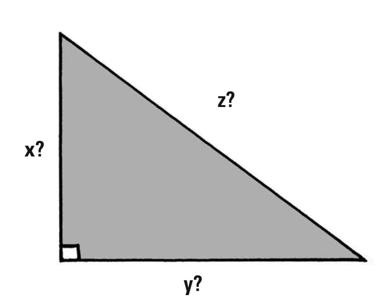
L'équation $x^2 + y^2 = z^2$ Nous allons maintenant examiner les carrés. Le carré d'un nombre est ce nombre multiplié par lui-même, et on l'écrit sous la forme x^2. Si $x = 3$, alors $x^2 = 3 \times 3 = 9$. L'équation dont il est maintenant question n'est plus $x + y = z$ mais

$$x^2 + y^2 = z^2.$$

Peut-on la résoudre comme précédemment, en choisissant des valeurs pour x et y et en calculant z ? Avec les valeurs $x = 3$ et $y = 7$, par exemple, le membre de gauche de l'équation est égal à $3^2 + 7^2$, soit $9 + 49 = 58$. Pour cela, z devrait être la racine carrée de 58 ($z = \sqrt{58}$), soit 7,6158 en valeur approchée. On peut certainement dire que $x = 3$, $y = 7$ et $z = \sqrt{58}$ sont solutions de $x^2 + y^2 = z^2$, mais malheureusement, les équations diophantiennes ne peuvent avoir pour solutions que des nombres entiers.

Comme $\sqrt{58}$ n'est pas un nombre entier, les valeurs $x = 3$, $y = 7$ et $z = \sqrt{58}$ ne conviennent pas.

L'équation $x^2 + y^2 = z^2$ est liée aux triangles. Si les valeurs de x, y et z représentent les longueurs des trois côtés d'un triangle rectangle, elles satisfont l'équation. Réciproquement, si x, y et z satisfont l'équation, alors l'angle formé par les côtés de longueurs respectives x et y est un angle droit. En raison de leurs liens avec le théorème de Pythagore, les solutions x, y et z sont appelées les triplets Pythagoriciens.



Comment trouver des triplets Pythagoriciens ? C'est là qu'intervient l'ouvrier du bâtiment. Parmi tout le matériel de l'ouvrier, figure l'équerre de dimensions 3, 4, 5. Il s'avère que les valeurs $x = 3$, $y = 4$ et $z = 5$ sont solutions car $3^2 + 4^2 = 9 + 16 = 5^2$. D'après la réciproque du théorème de Pythagore, un triangle dont les côtés ont des longueurs égales à 3, 4 et 5 est nécessairement

1843 Kummer affirme qu'il a prouvé le théorème, mais Dirichlet signale une faille.

1907 Von Lindemann affirme avoir une preuve, mais on démontre qu'elle est fausse.

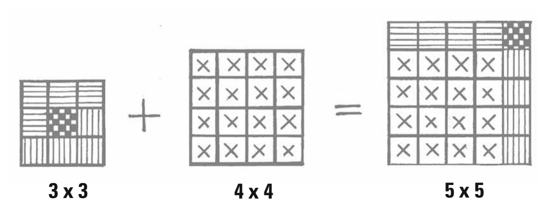
1908 Wolfskehl offre un prix pour toute solution obtenue avant 2008.

1994 Wiles finit par prouver le théorème.

rectangle. C'est l'outil mathématique que l'ouvrier utilise pour construire ses murs à angles droits.

Dans ce cas, on peut casser un carré 3×3 et se servir des morceaux pour les placer autour d'un carré 4×4 afin de construire un carré 5×5.

L'équation $x^2 + y^2 = z^2$ a des solutions entières. Par exemple, $x = 5$, $y = 12$ et $z = 13$ est une autre solution parce que $5^2 + 12^2 = 13^2$, et il y a en fait une infinité de solutions pour cette équation. La solution de l'ouvrier $x = 3$, $y = 4$ et $z = 5$ a la place d'honneur parce que c'est la solution la plus petite, et c'est la seule solution composée de nombres entiers consécutifs. Il y a de nombreuses solutions où deux nombres sont consécutifs, telles que $x = 20$, $y = 21$ et $z = 29$, mais aucune autre avec trois nombres consécutifs.



Après la fête, la famine On a l'impression que passer de $x^2 + y^2 = z^2$ à $x^3 + y^3 = z^3$ ne fait pas grande différence. Peut-on alors reprendre cette idée astucieuse qui consiste à rassembler un carré en morceaux autour d'un autre carré pour en former un troisième et l'appliquer à un cube ? Peut-on rassembler un cube autour d'un autre pour en construire un troisième ? Il s'avère que c'est impossible. L'équation $x^2 + y^2 = z^2$ a une infinité de solutions distinctes, mais Fermat a été incapable de trouver une seule solution pour $x^3 + y^3 = z^3$. Le pire était à venir, et Leonhard Euler, qui n'obtenait pas de résultats, fut amené à formuler la conjecture suivante :

L'équation $x^n + y^n = z^n$ n'a aucune solution entière pour toutes les valeurs entières de n supérieures ou égales à 3.

Pour démontrer ce théorème, on peut commencer avec des petites valeurs de n et poursuivre avec des valeurs supérieures. C'est ainsi que travailla Fermat. Le cas $n = 4$ est en réalité plus simple que $n = 3$, et Fermat avait probablement une preuve pour ce cas. Aux XVIIIe et XIXe siècles, Euler traita le cas $n = 3$, Adrien-Marie Legendre démontra le cas $n = 5$, et Gabriel Lamé prouva le cas $n = 7$. Au début, Lamé pensait avoir une preuve du théorème dans le cas général, mais il s'était malheureusement trompé.

Ernst Kummer apporta une contribution majeure à la résolution du problème. Ainsi, en 1843, il soumit un manuscrit dans lequel il affirmait avoir prouvé le théorème dans le cas général, mais Dirichlet signala qu'il y avait un manque dans son raisonnement. L'Académie des Sciences française offrit un prix de 3 000 francs à celui qui apporterait une preuve valide, et le décerna finalement à Kummer pour cet essai méritoire. Kummer prouva le théorème pour tous les nombres premiers infé-

rieurs à 100 (et d'autres valeurs) mais en excluant les nombres premiers irréguliers 37, 59 et 67. Par exemple, il ne réussit pas à démontrer qu'aucun entier ne satisfaisait l'équation $x^{67} + y^{67} = z^{67}$. Son échec à prouver le théorème dans le cas général permit l'essor de techniques précieuses dans la théorie algébrique des nombres. Ce fut peut-être une contribution aux mathématiques plus importante encore que de formuler le problème lui-même.

Ferdinand von Lindemann, qui réussit à prouver que la quadrature du cercle était impossible (voir p. 22), affirma qu'il avait prouvé le théorème en 1907 mais on découvrit qu'il s'était trompé. En 1908, Paul Wolfskehel légua par testament un prix de 100 000 marks au premier qui en apporterait une preuve dans les 100 ans à venir. Avec le temps, environ 5 000 preuves furent présentées, vérifiées puis retournées à leurs auteurs parce qu'elles étaient fausses.

La preuve Alors que le théorème de Pythagore ne s'applique qu'au cas $n = 2$, le lien avec la géométrie s'avéra être l'un des ingrédients incontournables de la preuve du théorème de Fermat. On a établi une relation avec la théorie des courbes elliptiques, et une conjecture fut proposée par deux mathématiciens japonais, Yutaka Taniyama et Goro Shimura. En 1993, Andrew Wiles fit une conférence sur cette conjecture à Cambridge et donna sa preuve du théorème de Fermat. Cette preuve contenait malheureusement une faille.

Le mathématicien français André Weil méprisait ces tentatives. Il compara la recherche d'une preuve de ce théorème à l'ascension de l'Everest ajoutant que, si un homme arrive à 100 mètres du sommet, il a échoué dans son ascension. Il avait mis la pression. Wiles s'isola et travailla sans relâche sur le problème. Beaucoup pensèrent que Wiles rejoindrait cette foule de gens qui étaient à deux doigts de réussir.

Avec l'aide de quelques collègues cependant, Wiles parvint à trouver l'erreur et à corriger le raisonnement. Cette fois, il put convaincre les experts et prouver le théorème. Sa preuve fut publiée en 1995 et il postula pour le prix Wolfskehl juste dans les temps pour se faire un nom dans le monde des mathématiques. Le petit garçon de dix ans qui lisait un livre sur ce problème à la bibliothèque des années plus tôt avait fait bien du chemin.

l'idée clé
Prouver un point marginal

50 L'hypothèse de Riemann

L'hypothèse de Riemann représente l'un des défis les plus coriaces des mathématiques pures. On a finalement réussi à venir à bout de la conjecture de Poincaré et du grand théorème de Fermat, mais pas de l'hypothèse de Riemann. Lorsqu'elle sera démontrée, d'une façon ou d'une autre, alors les problèmes les plus tenaces sur la distribution des nombres premiers seront résolus et engendreront un éventail de nouveaux problèmes qui seront autant de sujets de méditation pour les mathématiciens.

L'histoire commence avec l'addition de fractions du type

$$1+\frac{1}{2}+\frac{1}{3}$$

La réponse est 11/6 (soit en valeur approchée 1,83). Mais que se passe-t-il si l'on continue à additionner des fractions de plus en plus petites, par exemple 10 fractions de ce type ?

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10}.$$

En utilisant une simple calculatrice, la somme de ces fractions est égale en valeur approchée à 2,9. Un tableau montre comment le résultat total augmente à mesure que l'on ajoute des termes.

Nombre de termes	Valeurs (approchées)
1	1
10	2,9
100	5,2
1 000	7,5
10 000	9,8
100 000	12,1
1 000 000	14,4
1 000 000 000	21,3

La série de nombres

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\ldots$$

s'appelle une série harmonique. L'adjectif harmonique vient des Pythagoriciens qui pensaient que diviser la corde d'un instrument de musique par un demi, un tiers, et un quart donnait les harmoniques essentielles.

chronologie

1854
Riemann commence son travail sur la fonction zêta.

1859
Riemann prouve que les zéros non triviaux de $\zeta(s)$ se trouvent dans une bande critique et propose sa conjecture.

1896
De la Vallée-Poussin et Hadamard montrent que tous les zéros non triviaux se trouvent à *l'intérieur* de la bande critique de Riemann.

Dans la série harmonique, on fait la somme de fractions de plus en plus petites, mais que se passe-t-il pour le résultat total ? Devient-il supérieur à tous les autres nombres ou y a-t-il une limite quelque part, une limite qu'il ne peut jamais dépasser ? Pour répondre à cette question, l'astuce est de grouper les termes. Si l'on fait par exemple la somme des huit premiers termes (en sachant que $8 = 2 \times 2 \times 2 = 2^3$)

$$S_{2^3} = 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right)$$

(où S représente la somme) et, comme 1/3 est supérieur à 1/4 et 1/5 est supérieur à 1/8 (et ainsi de suite), la somme est supérieure à

$$1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}$$

On peut donc dire

$$S_{2^3} > 1 + \frac{3}{2}$$

et, plus généralement,

$$S_{2^k} > 1 + \frac{k}{2}$$

Si l'on prend $k = 20$, de sorte que $n = 2^{20} = 1\ 048\ 576$ (soit plus d'un million de termes), la somme de la série est seulement supérieure à 11 (voir le tableau). Le résultat augmente avec une lenteur effroyable, mais une valeur de k peut être choisie telle que la série augmente et atteigne ainsi n'importe quel nombre fixé à l'avance, quelle que soit sa taille. On dit que la série diverge vers l'infini. En revanche, ce n'est pas la même chose lorsque la série est constituée de termes élevés au carré :

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \ldots$$

On procède d'une manière similaire : on fait la somme de nombres de plus en plus petits, mais cette fois, une limite est atteinte, et cette limite est inférieure à 2. De façon inattendue, la série converge vers $\frac{\pi^2}{6} = 1{,}64493\ldots$

Dans cette dernière série, les termes sont élevés à la puissance 2. Dans la série harmonique, les dénominateurs sont tacitement élevés à la puissance 1 et cette valeur est critique. Si la puissance augmente très faiblement vers une valeur à peine supérieure à 1, la série converge, mais si la puissance est égale ou à peine inférieure à 1, la série diverge. La série harmonique, qui diverge, est à la transition entre convergence et divergence.

La fonction zêta de Riemann La célèbre fonction zêta de Riemann ζ était en fait connue d'Euler au XVIIIe siècle mais c'est Bernhard Riemann qui en reconnut

1900
Hilbert fait figurer l'hypothèse de Riemann dans sa liste des grands problèmes mathématiques non résolus.

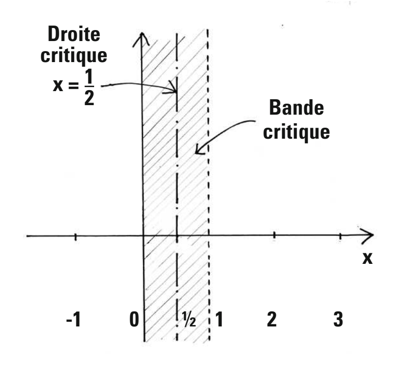
1914
Hardy prouve qu'il y a une infinité de solutions sur la droite critique.

2004
On démontre que les 100 milliards premiers zéros se trouvent sur la droite critique.

toute l'importance. Le symbole ζ correspond à la lettre grecque zêta, et la fonction s'écrit

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \ldots$$

On a calculé différentes valeurs de la fonction zêta, mais $\zeta(1) = \infty$ a surtout retenu l'attention parce que $\zeta(1)$ est la série harmonique. La valeur de $\zeta(2)$ est $\frac{\pi^2}{6}$, résultat découvert par Euler. On a montré que les valeurs de $\zeta(s)$ impliquent toutes π lorsque *s* est un nombre pair, alors que la théorie de $\zeta(s)$ pour des valeurs impaires de *s* est bien plus compliquée. Roger Apéry a prouvé le résultat important selon lequel $\zeta(3)$ est un nombre irrationnel, mais sa méthode n'a pas pu être appliquée aux valeurs $\zeta(5)$, $\zeta(7)$, $\zeta(9)$… ni aux valeurs suivantes.



L'hypothèse de Riemann La variable *s* dans la fonction zêta de Riemann représente une variable réelle mais elle peut représenter un nombre complexe (voir page 32). Cela permet de lui appliquer les techniques puissantes de l'analyse complexe.

La fonction zêta de Riemann comporte une infinité de zéros, c'est-à-dire une infinité de valeurs de *s* pour lesquelles $\zeta(s) = 0$. Dans un article présenté à l'Académie des Sciences de Berlin en 1859, Riemann a montré que tous les zéros non triviaux étaient des nombres complexes qui se trouvaient dans la bande critique délimitée par les droites d'équations $x = 0$ et $x = 1$. Il est aussi l'auteur de la célèbre conjecture :

Tous les zéros non triviaux de la fonction zêta de Riemann ζ(s) sont sur la droite critique d'équation $x = 1/2$, droite qui traverse la bande critique en son milieu.

La première avancée véritable vers la résolution de cette hypothèse fut faite indépendamment en 1896 par Charles de la Vallée-Poussin et Jacques Hadamard. Ils montrèrent que les zéros doivent se trouver à l'intérieur de la bande (et donc $\zeta(s)$ ne s'annule pas sur les droites $x = 0$ et $x = 1$). En 1914, le mathématicien anglais G. H. Hardy a prouvé qu'une infinité de zéros se trouvent sur la droite critique $x = 1/2$, même si cela ne peut empêcher le fait qu'une infinité de zéros puissent se trouver ailleurs que sur cette droite.

En ce qui concerne les résultats, les zéros non triviaux calculés en 1986 (1 500 000 000 de zéros) se trouvent bien sur la droite $x = 1/2$, alors que les résultats récents ont vérifié que les 100 milliards premiers zéros se situent également sur cette droite. Alors que ces résultats expérimentaux suggèrent que la conjecture est vraie, il reste la possibilité qu'elle soit fausse. La conjecture dit que tous les zéros se trouvent sur cette droite critique, mais encore faut-il le prouver ou l'infirmer.

Pourquoi l'hypothèse de Riemann est-elle importante ? Il y a un lien inattendu entre la fonction zêta de Riemann $\zeta(s)$ et la théorie des nombres

premiers (voir p. 36) Les nombres premiers sont des nombres uniquement divisibles par 1 et par eux-mêmes, tels que 2, 3, 5, 7, 11 et ainsi de suite. En utilisant les nombres premiers, on peut former l'expression

$$\left(1-\frac{1}{2^s}\right)\times\left(1-\frac{1}{3^s}\right)\times\left(1-\frac{1}{5^s}\right)\times\ldots$$

et il s'avère que, si l'on développe ce produit, on retrouve $\zeta(s)$, la fonction zêta de Riemann. Cela signifie que la connaissance de la fonction zêta de Riemann nous éclairera sur la distribution des nombres premiers et améliorera notre compréhension des composantes fondamentales des mathématiques.

En 1900, David Hilbert dressa la liste de ses célèbres 23 problèmes non résolus à l'adresse des mathématiciens. De son huitième problème, il dit : « Si je devais m'éveiller après avoir dormi pendant cinq cents ans, ma première question serait : l'hypothèse de Riemann a-t-elle été démontrée ? »

Hardy utilisa l'hypothèse de Riemann comme garantie pour traverser la mer du Nord lors d'une visite estivale à son ami Harald Bohr au Danemark. Avant de quitter le port, il envoya une carte dans laquelle il déclarait qu'il venait juste de prouver l'hypothèse de Riemann. Il était gagnant quoiqu'il arrive. Si le bateau avait coulé, il aurait eu l'honneur posthume d'avoir résolu le grand problème. D'un autre côté, si Dieu existait vraiment, il n'aurait pas laissé un athée tel que Hardy avoir cet honneur et aurait donc tout fait pour empêcher son bateau de couler.

Celui qui sera capable de résoudre ce problème avec rigueur gagnera un prix d'un million de dollars offert par l'Institut Mathématiques Clay. Mais l'appât du gain n'est pas ce qui motive la plupart de ces chercheurs qui, s'ils parvenaient à résoudre ce problème, s'assureraient une place d'honneur au panthéon des grands mathématiciens.



Glossaire

Algèbre. Remplaçant les nombres par des lettres pour étendre l'arithmétique, l'algèbre est aujourd'hui une méthode générale qui s'applique à toutes les branches mathématiques et leurs applications. Vient de « *al-jabr* » (reconstruction), mot apparu dans un texte arabe du IXe siècle.

Algorithme. Suite d'instructions à appliquer dans un ordre précis pour résoudre un problème.

Axiome. Proposition considérée comme vraie qui n'exige aucune démonstration et qui sert de base à une théorie mathématique. Le « postulat » des Grecs a la même fonction, mais il ne s'impose pas comme une évidence et n'est que provisoirement admis.

Base. Nombre de symboles utilisés dans un système de numération de position. Les Babyloniens avaient un système en base 60, alors que le système de numération moderne est en base 10 (système décimal).

Bijection. Nature de la relation entre deux ensembles lorsqu'à tout élément de l'ensemble de départ on associe un et un seul élément de l'ensemble d'arrivée.

Cardinal. Nombre d'éléments d'un ensemble fini. Le cardinal de l'ensemble $\{a, b, c, d, e\}$ est 5. Notion également définie pour les ensembles infinis.

Carré ou carré parfait. Produit d'un nombre par lui-même. Le nombre 9 est un carré parfait puisque $9 = 3 \times 3$.

Commutativité. La multiplication est commutative si $a \times b = b \times a$ (ex. : $2 \times 3 = 3 \times 2$). Ce n'est pas le cas dans de nombreuses branches de l'algèbre moderne (voir l'algèbre matricielle).

Contre-exemple. Exemple qui infirme une proposition. On démontre que la proposition « Tous les cygnes sont blancs » est fausse en exhibant un cygne noir, un contre-exemple.

Coordonnées. Idée de René Descartes consistant à utiliser un repère pour déterminer la position d'un point à l'aide de ses coordonnées x (par rapport à l'axe des abscisses) et y (axe des ordonnées).

Corollaire. Conséquence d'un théorème.

Dénominateur. Partie inférieure d'une fraction. Dans 3/7, le nombre 7 est dénominateur.

Dérivation. Opération fondamentale qui produit la dérivée. La vitesse est la dérivée du déplacement par rapport au temps, l'accélération celle de la vitesse par rapport au temps.

Diagramme de Venn. Représentation schématique (communément appelée « patate ») utilisée en théorie des ensembles.

Discret. Contraire de « continu ». Les valeurs discrètes sont séparées les unes des autres de la même manière que les entiers 1, 2, 3…

Diviseur. Entier qui en divise un autre avec un reste nul. Les nombres 2 et 3 sont les diviseurs de 6.

Ensemble. Collection, groupement d'objets appelés éléments : M = {chaise, table, canapé, tabouret, buffet} est par exemple un ensemble de meubles.

Ensemble vide. Ensemble qui ne contient aucun élément, noté Ø, utile en théorie des ensembles.

Équation diophantienne. Équation dont les coefficients et les inconnues ne peuvent être que des entiers ou des fractions, qui tient son nom de Diophante d'Alexandrie (vers 250).

Exposant. Notation utilisée en arithmétique indiquant le produit d'un nombre par lui-même. 5×5 s'écrit ainsi 5^2, 2 étant l'exposant. $5 \times 5 \times 5$ s'écrit 5^3, etc. Cette notation peut être élargie : $5^{1/2}$ signifie par $\sqrt{5}$. On emploie aussi le terme « puissance ».

Fraction. Nombre entier divisé par un autre.

Fractions unitaires. (ou égyptiennes) Fractions dont le numérateur est égal à 1. Le système de numération des Égyptiens de l'Antiquité reposait en partie sur elles.

Géométrie. Domaine traitant des propriétés des droites, des figures et des espaces, formalisé dans les *Éléments* d'Euclide au IIIe siècle av. J.-C. La géométrie est partout présente dans les mathématiques et a aujourd'hui perdu son sens historique restrictif.

Hypothèse. Proposition qu'on admet provisoirement et qui doit être prouvée ou infirmée. Elle a le même statut mathématique que la conjecture.

Intégration. Opération fondamentale pour la mesure des aires. Elle est parfois l'opération inverse de la dérivation.

Itération. Répétition d'un procédé de calcul à partir d'une valeur *a*.

Lemme. Proposition démontrée et utilisée comme résultat intermédiaire pour progresser dans la démonstration d'un théorème.

Loi de probabilité. Répartition des probabilités d'événements élémentaires dans une expérience aléatoire. La loi de Poisson donne les probabilités que *r* événements rares se produisent pour chaque valeur de *r*.

Matrice. Tableau de nombres ou de symboles disposés en carré ou en rectangle. On peut faire la somme ou le produit des tableaux qui forment un système algébrique.

Nombre premier. Entier supérieur ou égal à 2 qui n'est divisible que par 1 et par lui-même. Le nombre 7 est un nombre premier mais 6 n'en est pas un ($6 = 3 \times 2$).

Nombre transcendant. Nombre qui n'est pas solution d'une équation algébrique. Le nombre π est transcendant.

Nombre imaginaire. Produit d'un nombre réel par l'« imaginaire » i tel que $i^2 = -1$. Ils font partie des nombres complexes qui s'écrivent $a + ib$ avec a et b réels.

Nombre rationnel. Nombre qui peut s'écrire sous forme de fraction.

Numérateur Partie supérieure d'une fraction. Le nombre 3 est le numérateur dans la fraction 3/7.

Plan d'Argand-Cauchy. Représentation du plan à deux dimensions des nombres complexes.

PGCD. Le PGCD de deux nombres est le plus grand nombre qui les divise exactement l'un et l'autre. 6 est le PGCD de 18 et 84.

Polyèdre. Forme solide à plusieurs faces. Un tétraèdre a 4 faces triangulaires, un cube, 6 faces carrées.

Quadrature du cercle. Problème de construction à la règle et au compas d'un carré de même surface qu'un cercle de rayon donné, impossible à résoudre.

Quaternions. Nombres imaginaires à 4 dimensions découverts par W. R. Hamilton.

Racine carrée. Nombre qui, lorsque multiplié par lui-même, égale un nombre donné. 3 est la racine carrée de 9 car $3 \times 3 = 9$.

Reste. Dans la division euclidienne de a par b qui s'écrit $a = bq + r$, avec $0 \leq r \leq b$, r est le reste. Puisque $17 = 3 \times 5 + 2$, 17 divisé par 5 donne un reste de 2.

Rotation. Transformation d'un plan qui fait tourner les figures autour d'un point appelé centre, relativement à un angle.

Section conique. Désigne la famille classique de courbes incluant droites, cercles, ellipses, paraboles et hyperboles, toutes sections d'un cône par un plan.

Série Somme infinie d'une suite de nombres ou symboles.

Solution optimale. Pour de nombreux problèmes, il s'agit de trouver la meilleure solution ou solution optimale. Ce peut être celle qui minimise un coût ou maximise un profit par exemple.

Suite. Liste (souvent infinie) de nombres ou symboles.

Symétrie axiale. Transformation du plan par rapport à une droite appelée axe, telle que l'axe est la médiatrice entre tout point de la figure et l'image de ce point.

Système binaire. Système numérique en base deux utilisant les symboles 0 et 1. Joue un rôle important en informatique.

Système hexadécimal. Système numérique en base 16 utilisant les symboles 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, très utilisé en informatique.

Système de numération de position. La valeur d'un nombre dépend de la position des chiffres qui le composent. Dans « 73 », la position du chiffre 7 signifie « 7 dizaines » et celle du 3 « 3 unités ».

Théorème. Terme utilisé pour désigner un énoncé démontré aux conséquences importantes.

Théorème de Pythagore. Soit un triangle rectangle de côtés x, y et z, alors $x^2 + y^2 = z^2$, où z est la longueur du côté le plus long (l'hypoténuse).

Théorie du chaos. Théorie des systèmes dynamiques qui semblent aléatoires mais présentent une régularité sous-jacente.

Index

Les numéros de page en gras renvoient au glossaire

L'édition originale de cet ouvrage a été publiée en 2014 au Royaume-Uni
par Quercus Publishing Plc
sous le titre *50 Maths Ideas You Really Need to know*.

Originally entitled 50 Maths Ideas You Really Need to know.
First published in the UK by Quercus Publishing Plc

Photo p.101 © iStockphotos

Conseiller éditorial : Dominique Roux

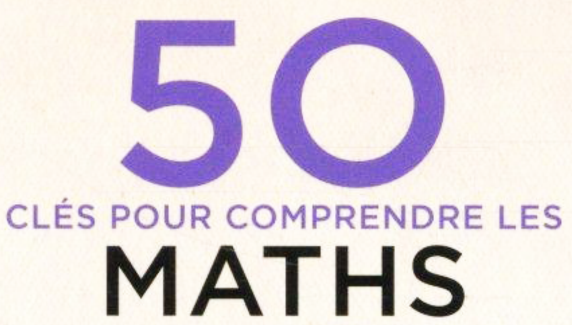
Dans la même collection :

50 clés pour comprendre l'astronomie, Joanne Baker
50 clés pour comprendre la physique, Joanne Baker
50 clés pour comprendre la physique quantique, Joanne Baker
50 clés pour comprendre les grandes idées de la science, Paul Parsons et Gail Dixon
50 clés pour comprendre l'architecture, Philip Wilkinson

Une précédente version a été publiée en 2008 sous le titre
« Juste assez de Maths pour briller en société »

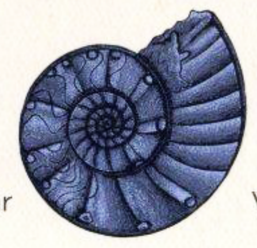
11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-076608-6



CLÉS POUR COMPRENDRE LES

MATHS



Traduit de l'anglais par Véronique Bordellès

Les mathématiques sont partout à l'œuvre dans notre vie quotidienne. Nous comptons, mesurons, additionnons à longueur de journée selon des règles bien établies.

Du zéro à la théorie des jeux, cet ouvrage présente 50 grandes idées à connaître en mathématiques. Sur quatre pages, agrémentée d'anecdotes historiques, d'exemples et d'illustrations, chacune peut se lire indépendamment des autres.

Tony Crilly est Professeur à l'université du Middlesex (Royaume-Uni).



3512250
ISBN 978-2-10-076203-3

15,90 € Prix France TTC

